LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Kuluttaja-asiakaspalvelun tietoturvallisen työskentelyn kehittäminen

Pehrsson Tom

2015 Tietojenkäsittelyn koulutusohjelma

Laurea-ammattikorkeakoulu
Leppävaara

Kuluttaja-asiakaspalvelun tietoturvallisen työskentelyn kehittäminen

Tom Pehrsson
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Lokakuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tom Pehrsson
Kuluttaja-asiakaspalvelun tietoturvallisen työskentelyn kehittäminen

Vuosi 2015 Sivumäärä 53

Opinnäytetyön tarkoituksena oli kartoittaa yrityksen X kuluttaja-asiakaspalvelun henkilöstön tietoturvatietoisuutta sekä listata mahdolliset riskitekijät, joihin kyseinen yksikkö altistuu päivittäisessä työtehtävissä tietojärjestelmiin sekä asiakasdatan käsittelyyn liittyen. Tavoitteena on kehittää kohdeyrityksen henkilöstöturvallisuutta sekä minimoida itse henkilöstön työskentelystä johtuvat riskitekijät. Yrityksen kehityskohteena on ollut itse henkilöstön perehdyttäminen, jonka vuoksi tämä opinnäytetyö toimii yrityksen kehittämistavoitteiden tukena.

Tämän tapaustutkimuksen päätavoitteena on tuottaa kohdeyritykselle tietoa tietoturvauhkista henkilöstön päivittäisessä työssä. Tiedon sekä prosessin tavoitteena on luoda tarkoituksenmukaiset ja tehokkaat tavat kohdeyrityksen henkilöstön tietoturvallisen työskentelyn kehittämiseen koulutuksien sekä perehdyttämisen muodossa.

Opinnäytetyö toteutettiin työelämälähtöisenä projektina, jossa teoreettisena viitekehyksenä toimii Valtiovarainministeriön VAHTI- ohjeistukset sekä kirjallinen materiaali. Työ koostui neljästä osasta, johon kuuluivat: haastattelut, tutkimus, koulutus sekä arviointi. Koko opinnäytetyö toteutettiin yhteistyönä yrityksen tietoturvapäällikön sekä kohdeyksikön johdon kanssa.

Teknisen tietoturvallisuuden keskiössä on tietojärjestelmien käyttäjät eli itse henkilöstö. Henkilöstöturvallisuuteen kohdistuvien riskitekijöiden taustalla suurimpana tekijänä on käyttäjän ajattelemattomuus tai riittämätön tietoturvallinen tietotaito.

Asiasanat, Henkilöstöturvallisuus, tietoturva, riskienhallinta, koulutus, oppiminen

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Programme in Business Information Technology

Tom Pehrsson
A Case Study of Improving Personnel Security for Customer Service

Year 2015 Pages 53

The purpose of this thesis is to find out personnel's information security awareness and find out risks which can occur in daily work. The objective of this thesis is to improve personnel to work more safely and minimize information security risks. This thesis is meant to be supporting Company X's needs to improve their personnel awareness which has been found as a development target.

The main object of this case study is to produce knowledge to the company X about possible information security risks within personnel. The object of the process and knowledge is to find out meaningful and efficient ways to improve personnel's work with the help of awareness training and introduction.

The thesis was completed as a work-oriented functional project in which theoretical framework was based on the VAHTI- instructions of the Ministry of Finance and on literature. This project includes four parts which are interviews, research survey, awareness training and evaluation. The thesis was executed by co-operating with Company X's Information Security Manager and target unit's management team.

The core of technical information security is information systems users (personnel).The risk factors for personnel's information security are mostly thoughtlessness or insufficient know-how of information security.

Keywords, personnel security, risk management, learning, awareness training

Sisällys

1 Johdanto

Tietoturvallinen ajattelutapa on liiketoiminnan sekä tietojärjestelmien keskeinen osa-alue, koska nykypäivänä lähes jokainen yritys on riippuvainen erilaisista tietojärjestelmistä. Henkilöstön päivittäin käsittelemät tiedot ovat yritykselle luottamuksellisia, jonka vuoksi tiedon arvo on huomattava. Tiedon ajantasaisuuden, luottamuksellisuuden tai eheyden katoaminen voi aiheuttaa yritykselle taloudellisia tappioita. Tämän takia yrityksen tulee suunnitella liiketoimintaprosessinsa samanaikaisesti tehokkaasti mutta myös tietoturvallisesti. Tietoturvallisuuteen kuuluu teknisen puolen lisäksi myös hallinnollinen puoli, jossa pääosassa on itse henkilöstö.

Tämän opinnäytetyön tarkoituksena on kartoittaa kohdeyrityksen kuluttaja-asiakaspalveluyksikön henkilöstön tietoturvallisuuden tämänhetkistä tasoa sekä löytää mahdolliset uhkakuvat asiakaspalvelun jokapäiväisestä tekemisestä. Kartoituksen jälkeen keskitytään löydettyjen uhkien minimoimiseen sekä henkilöstön yleisen taitotason parantamiseen. Tavoitteena on saada henkilöstö toimimaan yhtä tehokkaasti, mutta siinä samalla tietoturvallisesti.

Suurin uhka kohdeyritykselle on asiakaspalvelun käsittelemien asiakastietojen menettäminen tai joutuminen vääriin käsiin. Asiakastietojen menetys tai joutuminen vääriin käsiin voi aiheuttaa huomattavaa tuhoa liiketoiminnalle niin taloudellisesti kuin imagon näkökulmasta. Tällä kehittämistyöllä on tarkoitus vähentää asiakastietojen menettämisen uhkaa ohjeistamalla loppukäyttäjät (henkilöstö) työskentelemään tietoturvallisemmin.

Vaikka työ toteutetaan erityisesti kohdeyrityksen kuluttaja-asiakaspalvelua varten, tarkoituksena on myös soveltaa varsinaista tapaa suorittaa työ yrityksen toisiin yksiköihin. Työ edesauttaa myös henkilöstön tietoturvan lisäämistä muissa vastaavissa olosuhteissa. Tietoturvakoulutuksen materiaalin valmistaminen sekä koulutuksen pitäminen toimivat hyvänä mallina myös muihin vastaaviin tarpeisiin.

Opinnäytetyö jakautuu teoriapohjaan, tutkimukseen sekä varsinaiseen toteutukseen, johon kuuluu koulutusmateriaalin suunnittelu, valmistus sekä henkilöstön varsinainen kouluttaminen. Koulutusten jälkeen kerätään palautetta suoraan henkilöstöltä. Opinnäytetyön aihe tuli suoraan kohdeyritykseltä. Ulkopuolinen tekijä on suorittanut arvion yrityksen tietoturvallisuudesta syksyllä 2014, jossa todettiin, että yrityksen tulisi kehittää henkilöstönsä tietoturvatietoisuutta.

Teoriapohjassa keskitytään hallinnollisen tietoturvan yleiseen kuvaan suoraan tietoturvan viitekehyksen avulla. Valtiovarainministeriön VAHTI- julkaisut toimivat viitekehyksenä varsinai-

selle teoriapohjalle sekä henkilöstön tietoturvariskien arvioimisesta sekä itse henkilöstön kouluttamisesta. Tämän lisäksi apuna käytetään lähteenä myös kirjallisuutta.

Tutkimusvaiheessa tieto kerättiin haastatteluiden, systemaattisen havainnoinnin sekä tutkimuslomakkeen avulla. Tutkimuslomakkeen valmistus tapahtui yhdessä yksikön johtoryhmän kanssa. Toteutusvaiheessa valmistetaan tietoturvakoulutusta varten koulutusmateriaali, joka muokataan luokkakoulutuksia varten sekä luettavaksi online-muotoon suoraan yksikön sivuille. Koulutusta suunniteltaessa perehdytään koulutuksiin sekä oppimiseen liittyvään pedagogiikkaan, jotta kouluttamisella saadaan mahdollisimman hyvä lopputulos aikaiseksi. Materiaalissa otetaan huomioon kohdeyleisön ikä sekä koko, jonka vuoksi materiaalista pitää saada mahdollisimman helppolukuinen sekä mielenkiintoinen. Toteutuksen jälkeen tapahtuva palautteenkeruu suoritetaan yhdessä kohdeyrityksen johdon kanssa.

1.1 Työn tausta ja lähtökohdat

Opinnäytetyön pääviitekehyksenä toimii VAHTI- ohjeistukset. VAHTI on tietoturvallisuuden kehittämisen, ohjaamisen ja koordinaation elin, joka on ministeriön asettama johtoryhmä.

Tietotekniikan kehittyminen sekä tietojärjestelmistä syntynyt riippuvuus ovat aiheuttaneet sen, että tietoturvallinen ajattelutapa on lisääntynyt huomattavasti. Tämän vuoksi etenkin henkilöstö on yhä enemmän tietoturvallisuuden keskiössä. Yritykset tehostavat henkilöstönsä tietoturvaosaamiseen jatkuvasti, jotta mahdollisilta tietoturvauhkilta säästyttäisiin. Yrityksen henkilöstön tietoturvaa ohjaa yrityksen tietoturvapolitiikka. Henkilöstön kehittäminen, henkilöstöasioiden hallinta sekä johtaminen suunnitelmallisesti sekä järjestelmällisesti ovat keskeistä nykypäivän henkilöstöturvallisuudessa. Tietoturvarikkomuksista miltei jopa puolet liittyy henkilöstön organisaation menettelytapoihin. Henkilöstön jokapäiväisen tekemisen tulisi olla tehokkuuden lisäksi myös turvallista. (VAHTI 2008.)

Henkilöstön tietoturvallisen käyttäytymisen ohjeistaminen sekä tiedostaminen on yrityksen johdon vastuulla. Tietoturvan taso riippuu pitkälti siitä, mitä varsinainen työnkuva pitää sisällään eli kuinka arkaluontoista materiaalia työntekijät työtehtävissään käsittelevät. Yritysten on arvioitava tietoturvaa CIA:n mallilla: tiedon luotettavuutta (Confidentiality) -eheyttä (Integirty), sekä -saatavuutta (Availability) henkilöstön työnkuvassa. Mittaaminen ja kartoitus ovat kuitenkin huomattavasti haastavampia henkilöstöön kohdistuvassa tietoturvallisuudessa kuin muissa tietoturvan osa-alueissa.

Opinnäytetyössä luodaan kuluttaja-asiakaspalvelun kautta mallipohja henkilöstöön kohdistuvan tietoturvan parantamiseksi. Kohdeyksikkö toimii pilottina yrityksen laajempaa henkilöstöturvallisuutta silmällä pitäen. Yrityksessä on havaittu henkilöstöturvallisuus yhtenä kehitys-

kohteena, jonka vuoksi tämä työ tukee huomattavasti yrityksen tarpeita henkilön päätetyöskentelyn tietoturvallisuuden parantamiseksi. Tutkija ehdotti kohdeyritykselle viitekehystä työlleen Valtiovarainministeriön VAHTI- ohjeistuksen mukaisesti. Koko opinnäytetyön toiminnallinen prosessi tutkimuksen suunnittelusta itse koulutusvaiheeseen rakennetaan VAHTI- ohjeistuksien mukaisesti.

1.2 Kohdeyrityksen sekä –yksikön esittely

Opinnäytetyö toteutettiin yhteen Suomessa media-alan konserniin. Yrityksen pyynnöstä opinnäytetyössä ei esitetä kyseisen yrityksen nimeä. Yritys toimii useassa Euroopan maassa. Yrityksen tuotevalikoimaan kuuluu tuotteita jokaiselta median osa-alueelta. Palveluita tuotetaan muun muassa televisioon, radioon, printtimediaan sekä internetiin.

Kohdeyksikkönä toimii konsernin suurimpien ja tunnetuimpien tuotteiden kuluttaja-asiakaspalvelu johon kuuluu kaiken kaikkiaan yhteensä 154 henkilöä. Tuotevalikoimaan kuuluu yhteensä miltei 40 tuotetta. Tuotevalikoimaan kuuluu sekä printtimediaa että digitaalisia tuotteita. Kuluttajien arvokkaimmat tuotteet pyörivät noin 400-500 euron hintaluokissa. Asiakkaita on kokonaisuudessaan toista miljoonaa. Kuluttaja-asiakaspalvelu käsittelee päivittäin toista tuhatta asiakaskontaktia. Asiakaspalvelu käsittelee tilauksia, maksutietoja sekä on päivittäin tekemisissä tuotteiden toimittamiseen sekä tuottamiseen toimivien yhteistyökumppanien kanssa.

Kohdeyksikön voi jakaa yhteensä neljään osaan, joissa käytetään erilaisia tietojärjestelmiä. Jokaisella osa-alueella on oma vastaava henkilö eli päällikkö. Tämän lisäksi asiakaspalvelussa on oma resurssienhallinta- sekä valmennusryhmä joihin kuuluu yhteensä 8 henkilöä. Asiakaspalvelussa on yhteensä 8 tiimiä, johon kuuluu noin 10-15 työntekijää sekä esimies eli ryhmänvetäjä. Jokaisessa tiimissä on osaajia jokaiselle asiakaspalvelun neljälle osa-alueelle.

Kohdeyksikössä henkilöstö käsittelee päivittäin isoja määriä erilaisia asiakastietoja sekä kontakteja. Asiakastietoja käsitellään esimerkiksi maksujen, tilausten sekä tuotteiden toimituksen osalta. Erilaisia asiakastietoja käsitellään pääosin sähköisten työkalujen välityksellä. Kuitenkin on havaittu, että työntekijät käyttävät myös paperia asiakastietojen välittämiseen sekä tallentamiseen.

1.3 Työn tarkoitus ja tavoitteet

Tarkoituksena on tehdä kehittämistyö, joka toimii yrityksen tietoturvatoimintaa edistävänä tekijänä. Työllä on tarkoitus luoda yritykselle malli henkilöstön tietoturvan parantamiseksi,

jota voidaan käyttää runkona koko henkilöstön kouluttamiseen. Tutkimuksen pohjalta on tarkoitus tarkastella asiakaspalvelun henkilöstöön kohdistuvia riskitekijöitä sekä suunnitella koulutus- sekä sen materiaali tavalla, joka minimoi havaitut uhkakuvat.

Tämän työn tavoitteena on tuoda yrityksen kuluttaja-asiakaspalvelun henkilöstölle tarvittavat tiedot sekä taidot tietoturvalliseen tekemiseen yrityksen tietoturvapolitiikan mukaisesti. Tavoitteena on tuoda keskeisimmät asiat tietoturvasta jokaiselle käyttäjälle jokapäiväiseen tekemiseen. Samalla tavoitteena on luoda kohdeyksikölle tietoturvaan liittyvä ohjeistus, jota käytetään tulevaisuudessa uusien työntekijöiden kouluttamiseen.

2 Henkilöstöturvallisuus

Suurin tietoturvavahingon aiheuttanut tekijä on henkilöstön ajattelemattomuus, tietämättömyys tai ohjeiden rikkominen. Ihminen on siis ehdottomasti tärkein tekijä, jopa tekniikan edellä. Tietoturvallinen työskentely on työntekijän vastuulla, jolloin sen toteutuminen riippuu jokaisesta yksilöstä. (VAHTI 2006.)

Huonosti hoidettu tai heikosti toteutettu tietoturva aiheuttaa haittaa niin yrityksen liiketoiminnalle kuin myös itse imagoon. Tietoturvan keskeinen asema on vasta viime vuosina saanut yritykset mukaansa. Etenkin maine sekä asiakkaiden sekä sijoittajien luottamus on jopa tärkeämpää kuin itse tietojärjestelmien sisältämät tiedot. (Laaksonen ym. 2006, 19; tietoturvaopas.fi.) Huonosti tietoturvallisuuttaan harjoittava yritys ei rohkaise yhteistyökumppaneita harjoittamaan liiketoimintaa, koska se tuottaa mahdollisia riskejä tietojen paljastumiseen ulkopuolisten käsiin.

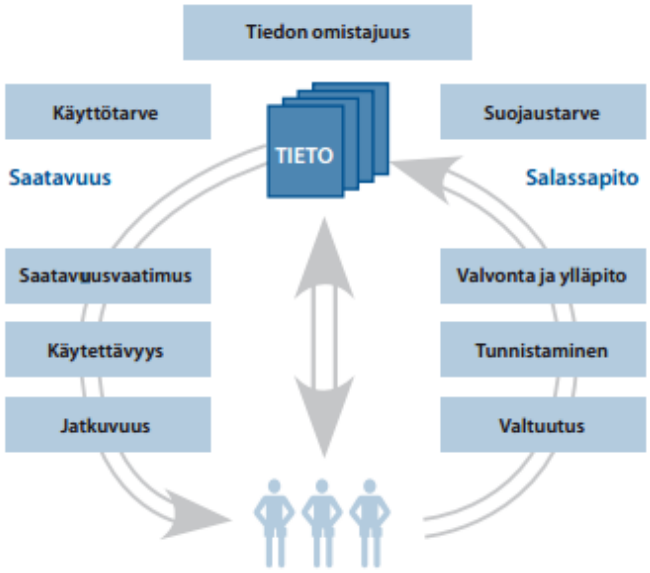
Laaksonen (2006) kertoo kirjassaan, että yritykset ovat lähes aina riippuvaisia tietietojärjestelmistään, jonka vuoksi jokainen henkilöstön jäsen on vastuussa tietoturvallisesta käyttäytymisestä. Tekniset sekä fyysiset tietoturvaratkaisut eivät ole tietoturvallisuuden takaavia asioita, koska viimekädessä vastuussa on itse ihminen eli tekijä, joka käyttää teknisiä järjestelmiä. Tietoturvallisuuden tasoa voidaan kehittää panostamalla etenkin ihmisten asenteisiin sekä varsinaisiin toimintatapoihin, joilla tietojärjestelmiä käytetään.

Tietoturvallisuudessa keskitytään yhä enemmän ja enemmän henkilöstöön sekä heidän kykyynsä työskennellä tietoturvallisella tavalla eli käsittelemällä työssään tarvittavaa tietoa turvallisesti. Tämän vuoksi yritykset ovat kokoajan tehostamassa tietoturvaosaamistaan henkilöstön kautta. Henkilöstön tietoturvallinen työnteko on yrityksen näkökulmasta erittäin tärkeässä asemassa yrityksen maineen sekä taloudellisten syiden vuoksi. (VAHTI 2008.)

Toisin kuin henkilöturvallisuudessa, henkilöstöturvallisuudessa keskitytään henkilöstöstä aiheutuvien riskien hallintaan sekä ennaltaehkäisemiseen. Henkilöstöturvallisuus onkin yksi osa yleisempää turvallisuuskäsitettä. Henkilöstöturvallisuutta, käytetään yleisen tietoturvallisuuden alaterminä. Sillä tarkoitetaan henkilöstöön liittyvien käytettävyysriskien hallintaa tietojärjestelmien ja tietojen osalta. Tähän kuuluu myös salassapitovelvollisuus. Tietojen turvaaminen henkilöstön toimesta on erittäin keskeinen asia henkilöstöturvallisuudessa. Suurin haaste henkilöstöturvallisuudelle on itse ihminen. Henkilöstö käsittelee yrityksen erilaisia tietoja monella eri tavalla esimerkiksi vastaanottamalla, muokkaamalla, tallentamalla, välittämällä sekä tuhoamalla. Henkilöstö ylläpitää myös tietoa sekä tietojärjestelmiä. (VAHTI 2008).

Henkilöstöturvallisuuteen sisältyy kaksi vaatimusta, jotka ovat riippuvaisia toisistaan. Ne ovat käytettävyysvaatimus ja tietojen eheysvaatimus sekä salassapitovaatimus. Tietoa voi esimerkiksi lähettää tai monistaa ilman alkuperäisen tiedon katoamista. Samalla kyseinen tieto on kuitenkin mahdollista hävittää tai kadottaa vahingossa. Yrityksien erilaisten tietojen määrä on erittäin suuri, jonka takia tiedon turvallisesta käsittelystä sekä hallinnasta on tullut keskeinen haaste organisaation toiminnalle. (VAHTI 2008.)

.



Taulukko 1 Henkilöturvallisuuden haaste suojata tietoja ja turvata sen saanti

3 Tutkimuksen toteutus ja tulokset

Alkuperäinen arvio henkilöstöön liittyvästä tietoturvaosaamisesta ja sen kehittämisestä on tullut jo viime syksynä ulkopuolisen tekijän toimesta, jossa todettiin henkilöstön toimintamalleissa tietoturvallisuuteen liittyviä puutteita. Yrityksellä oli siis tarve saada henkilöstön tietoturvaosaamisesta selkeää kuvaa, jonka vuoksi tutkija sai hyvät lähtökohdat varsinaiseen opinnäytetyöhön liittyen suoraan yrityksen toimesta. Kuluttaja-asiakaspalvelu toimisi näin ollen

ikään kuin pilottina koko yrityksen henkilöstön tietoturvan kartoittamisessa sekä kouluttamisessa.

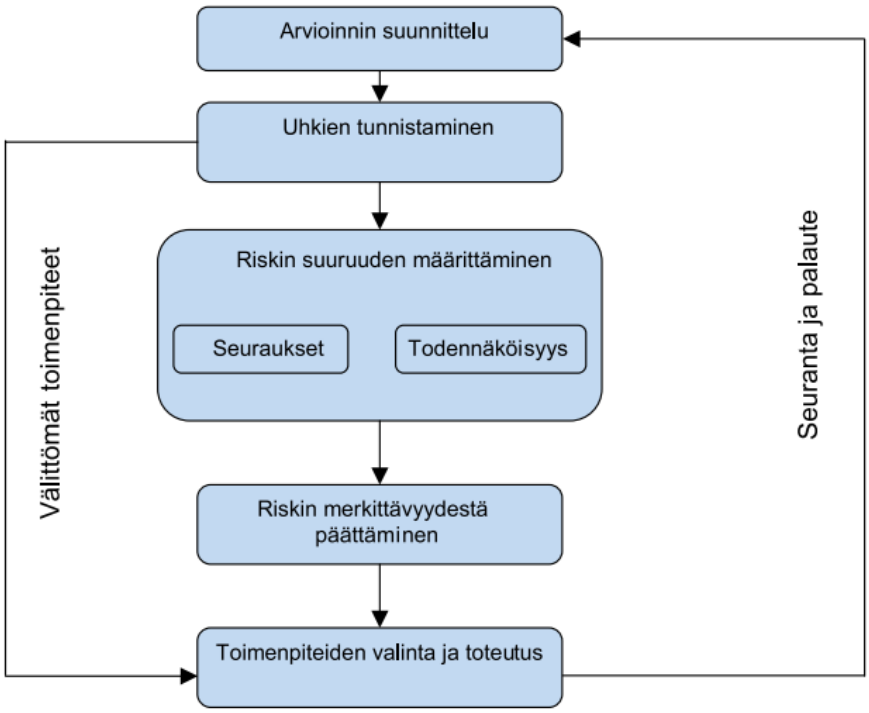
Ennen varsinaisen tutkimuksen valmistamista tutkija tapasi yrityksen tietoturvapäällikön sekä kohdeyksikön johdon. Tapaamisissa oli tarkoituksena käydä yleistä keskustelua siitä, mitkä jokapäiväisessä tekemisessä tapahtuvat asiat voisivat vaikuttaa yksikön tietoturvallisuuteen. Tapaamiset toimivat alustavan arvioinnin suunnitteluna, jonka jälkeen tutkija pääsi tutkimaan ja tunnistamaan uhkia tutkimuslomakkeen avulla (Taulukko 1). Tutkimus toteutettiin yhdessä tietoturvapäällikön sekä kuluttaja-asiakaspalvelun johdon kanssa. Keskustelu sekä uhkakuvien kartoitus tapahtui avoimena keskusteluna nk. ”aivoriihi”-mallilla, jossa havaittiin, että asiakaspalvelun henkilöstö kohtaa päivittäisessä työssään sekä ulkoisia, että sisäisiä riskejä.

Tämän lisäksi tutkija käytti tutkimusmenetelmänä systemaattista havainnointia, jossa tutkija seurasi kahden viikon ajan kohdeyksikön henkilöstön toimia jokapäiväisessä työssä. Havainnoinnin tuloksia analysoitiin yhdessä kohdeyksikön johdon sekä tietoturvapäällikön kanssa sovituissa palavereissa. Havaintojen perusteella saatiin selkeä määrä mahdollisista väärinkäytöksistä päätetyöskentelyssä tietoturvan näkökulmasta.

3.1 Haastatteluiden suunnittelu

Haastattelut suunniteltiin siten, että kohdeyksikön jokaisen osa-alueen vastaavat henkilöt olivat paikalla. Tämän lisäksi haastatteluun osallistui kohdeyksikön kouluttajat. Toinen haastattelu käytiin kahden kesken yrityksen tietoturvapäällikön kanssa. Keskusteluihin osallistuivat kaiken kaikkiaan yhteensä 10 henkilöä. Tarkoituksena oli saada haastatteluun joukko henkilöitä, jotka vastaavat kunkin kuluttaja-asiakaspalvelun osa-alueesta, jotta tarvittava tieto saataisiin oikealta taholta esiin. Tutkija toimi siis ikään kuin kohdeyksikön sekä tietoturvapäällikön välissä.

Haastatteluiden tavoitteena oli tutkia osaston työskentelytapoja sekä kartoittaa yleisimpiä riskejä henkilöstön päätetyöskentelyyn liittyen.



Kuva 1 Riskienhallinnan ja arvioinnin vaiheet (VAHTI 2003)

3.2 Haastattelut sekä tutkimuslomakkeen suunnittelu

Ennen varsinaisen tutkimuslomakkeen valmistamista tutkija kävi tapaamassa ensimmäisenä kohdeyksikön johtoa, jotta yleinen käsitys yksikön työnkuvasta käytännössä. Tutustuminen työnkuvaan sekä haastattelut auttoivat huomattavasti saamaan tarkempia kuvia siitä, mitä kukin asiakasneuvoja työssään päivittäin tekee asiakaskontakteissa. Tutkija sai samalla yleisen kuvan yhteisistä työkaluista, jonka avulla riskienkartoitusta päästiin tekemään entistä syvällisemmin.

Yksikköön tutustumisen jälkeen tutkija haastatteli tietoturvapäällikköä, jonka kanssa käytiin läpi mahdollisia uhkakuvia sekä kerrattiin läpi asioita, jotka tutustumiskierrokselta saatiin käsiin. Keskustelujen edetessä suurimmiksi uhkakuviksi esiintyivät etenkin kalasteluyritykset (Phishing) joihin henkilöstö altistui päivittäin työssään. Kalasteluyrityksinä toimii useimmiten sähköpostiviestit, joissa vaadittiin käyttäjältä tietoja tai lähetettiin ylimääräisiä liitteitä viestin ohessa. Tämän lisäksi yleinen henkilöstön ajattelemattomuus tietoturvanäkökulmasta katsottuna jokapäiväisessä käyttäytymisessä koettiin asiaksi, josta on hyvä puhua kohdeyksikön työntekijöiden kanssa. Tähän hyvänä esimerkkinä toimii tutkijan havainnot siitä, että työntekijät harvemmin lukitsivat työpistettään poistuessaan paikalta.

Tutkija suunnitteli lomakkeen Valtionvarainministeriön valmistaman Henkilöstön tietoturvaohjeen avulla (2013), jossa mainittiin yleisimpiä henkilöstöön liittyviä riskejä, jotka pääosin joh-

tuvat suoraan huolimattomuustekijöistä. Lomakkeen tarkoituksena oli saada vahvistus haastatteluissa sekä tutkijan havainnoista ilmenneistä epäilyksistä tietoturvallisessa käyttäytymisessä. Ennen varsinaisia toimenpiteitä tietoturvapäällikkö sekä asiakaspalvelun johto halusivat saada vahvistukset yleisille epäilyksille tutkimuslomakkeen tuloksien avulla.

3.3 Tutkimuslomake

Tutkimuslomake valmistettiin pääosin kvantitatiivisin kysymyksin, koska tutkija sai haastatteluiden avulla selkeän kuvan siitä, että yleinen tietoturvaosaaminen oli erittäin vähäistä, jonka vuoksi kvalitatiivisten kysymysten kysyminen henkilöstöltä olisi epäkäytännöllistä. Tutkimuskyselyn tarkoituksena on tunnistaa mahdolliset uhkakuvat jatkotoimenpiteitä varten (Taulukko 2).

Tutkimuksella haluttiin saada tietoon yleisempien päätetyöskentelyyn liittyviä tietoturvauhkia sekä arvioida niiden toteutumista kohdeyksikössä. Tutkimuksen tarkoitus oli vahvistaa tutkijan sekä yksikön johdon asettamat epäilyt henkilöstön tietoturvatietoisuuden tasosta. Tutkimuslomake löytyy opinnäytetyön liitteistä (Liite 1). Seuraavassa on kerrottu kysymyskohtaisesti syitä sille, minkä takia asiaa kysyttiin tutkimuksessa:

Kysymys yksi: Oletko tietoinen yrityksen yleisestä tietoturvapolitiikasta?

Kohdeyrityksellä on käytössään yleinen ohjeistus tietoturvalliseen käyttäytymiseen. Kyseinen ohjeistus on kuitenkin asetettu paikkaan, josta harva työntekijä sitä löytää. VAHTI- ohjeistuksen mukaisesti yrityksen näyttää oma tietoturvaohjeistuksensa selvästi, jotta ohjeistus olisi työntekijöiden saatavilla. Kohdeyrityksen tietoturvapäällikön mukaan kyseisen ohjeistus tulisi olla selvemmin esillä. Tutkija oli haastatteluissa saanut selkeä kuvan siitä, että kohdeyksikön henkilöstöllä ei ole selkeää kuvaa siitä, mikä on yrityksen yleinen laita tietoturvaan liittyen. Tämän lisäksi tietoturvallisesta työskentelystä ei ole haastatteluiden mukaan ollut tarpeeksi ohjeistusta henkilöstölle.

Kysymys kaksi: Oletko lukenut yrityksen yleisen tietoturvaohjeistuksen?

Kysymyksen tarkoituksena oli saada täsmällisempi määrä, kuinka moni on lukenut yrityksen yleisen tietoturvaohjeistuksen. Haastatteluissa ilmeni, että yrityksellä on olemassa yleinen tietoturvaohjeistus, mutta se löytyi ainoastaan englanninkielisenä. Tämän lisäksi kyseinen ohjeistus oli varsin hyvin ”piilotettu”, jonka takia sitä oli erittäin hankala löytää.

Kysymys kolme: Onko työnantaja antanut sinulle tarvittavan ohjeistuksen/ koulutuksen tietoturvaan liittyen?

Tutkija haastatteli kohdeyksikön johtoa sekä tietoturvapäällikköä, jossa selvisi, että tietoturvaohjeistuksissa on havaittu puutteita. Tämä esiintyy etenkin ohjeistuksen saatavuudella. VAHTI- ohjeistuksen (4/2013) mukaan tietoturvaohjeistuksen tulisi olla osa henkilöstön perehdytystä, jolloin mahdolliset uhkat henkilöstön toimesta voidaan minimoida. Kysymyksellä oli tarkoituksena saada henkilöstön oma mielipide selville siitä, onko yritys antanut tarpeeksi ohjeistusta tietoturvalliseen tekemiseen.

Kysymys neljä: Käytätkö työpisteesi salasanaa muissa palveluissa (kuten Facebookissa tai Gmailissa)?

Kysymys viisi: Oletko kirjoittanut työpisteesi salasanan ylös muistiin?

Kysymyksen numero neljä tarkoituksena oli saada tietoa siitä, käyttääkö henkilöstö samaa salasanaa useassa eri paikassa. VAHTI- ohjeistuksen (2008) mukaisesti työsalasanaa tai tunnusta ei saisi koskaan käyttää muissa palveluissa. Mahdollisen tietomurron tapahtuessa työsähköposti sekä työpisteen salasana on erillään, jonka vuoksi esimerkiksi henkilökohtaisen sähköpostin tietomurto ei vaikuta työtunnuksiin.

Kysymys numero viisi koski salasanan kirjoittamista ylös muistiin. Tutkija havaitsi kohdeyksikön työpisteillä tarralappuja, joissa oli merkittynä kirjautumistunnukset sekä salasanat. Tämä asia esitettiin myös haastatteluiden yhteydessä, jonka vuoksi asialle tuli saada vahvistus. VAHTI- ohjeistuksen (2013) sekä yrityksen omien salasanakäytäntöjen mukaisesti salasanan tulisi olla uniikki ja vaikeasti arvattavissa, mutta tästä huolimatta se tulisi muistaa ulkoa. Etenkin salasanan kirjoittaminen ylös muistiin on tietoturvauhka, joka mahdollistaa salasanan väärinkäytön, jos tiloissa liikkuu esimerkiksi ylimääräisiä henkilöitä.

Tutkijan haastateltua tietoturvapäällikköä ilmeni, että yleisistä salasanakäytännöistä olisi hyvä tehdä ohjeistus koulutuksiin. Tämän vuoksi salasanakäytänteet päätettiin toiseksi pääaiheeksi koulutuksien sisällössä.

Kysymys kuusi: Lukitsetko työpisteesi aina poistuessasi paikaltasi?

Kysymyksellä oli tarkoitus saada loppukäyttäjiltä tietoa työpisteen lukitsemisesta aina paikalta poistuessa. Yrityksen yleisissä pelisäännöissä (Liite 4) on selkeästi mainittu, että oma työpiste tulisi sulkea aina poistuessaan paikaltaan. Tämän lisäksi myös VAHTI- ohjeistuksessa (2008) on selkeä maininta asiasta.

Tutkija havaitsi, että työntekijät jättivät jatkuvasti työpisteensä lukitsematta, kun he poistuivat paikaltaan. Kohdeyksikön tiloissa liikkuu myös satunnaisesti ulkopuolisia ihmisiä, joilla on mahdollisuus päästä käsiksi työpisteisiin. Tämän vuoksi kyseiseen aiheeseen tulee panostaa, jotta henkilöstö toimisi jatkossa oikein.

Kysymys seitsemän: Käytätkö työsähköpostiasi muihin asioihin (kuten esimerkiksi uutiskirjeisiin)?

Tavoitteena oli saada käyttäjiltä tietoa siitä, käyttävätkö he työsähköpostiaan muihin palveluihin rekisteröitymiseen tai uutiskirjeisiin. Tutkijan havainnot sekä haastatteluiden tulokset antoivat selkeästi viitettä siitä, että työntekijät käyttävät sähköpostejaan myös muuhun kuin työntekoon. Tähän haluttiin saada varmistusta tutkimustuloksien avulla. Sähköpostin käyttäminen muissa palveluissa voi altistaa kalasteluyrityksille, mikäli esimerkiksi uutiskirjeen vastaanottajalistat joutuvat vääriin käsiin. (VAHTI 4/2013)

Kysymys kahdeksan: Oletko ladannut työkoneellesi ylimääräisiä ohjelmia ilman lupaa?

Kysymys yhdeksän: Oletko liittänyt ylimääräisiä laitteita työkoneellesi (esimerkiksi usb- muistitikun tai matkapuhelimen)?

Kysymyksen numero kahdeksan selitys: Haastatteluissa ilmeni tieto siitä, että työkoneille ei pitäisi olla mahdollista ladata ylimääräisiä ohjelmia, koska ne vaativat käyttöjärjestelmän valvojan luvan. Tästä huolimatta tutkija halusi saada tiedon mahdollisista väärinkäytöksistä..

Kysymyksen numero yhdeksän selitys: Yrityksen yleiset pelisäännöt kieltävät ylimääräisten laitteiden kuten esimerkiksi USB- laitteiden ja matkapuhelimien liittämisen työkoneelle. Tästä huolimatta tutkija oli havainnut vastaavaa käytöstä kohdeyksikön tiloissa. Mikäli USB- laite tai matkapuhelin on saastunut, ylimääräinen laite saastuttaa mahdollisesti jokaisen koneen, johon laite liitetään. Ohjelmien lataus työpisteille altistaa latausten yhteydessä mahdollisten haittaohjelmien leviämisen. (VAHTI 4/2013).

Kysymys 10: Oletko saanut työsähköpostiisi viestejä tuntemattomalta lähettäjältä (esim. mainoksia tai liitetiedostoja)?

Kysymys 11: Oletko törmännyt epäilyttäviin sähköposteihin yleisen työkalun (asiakashallintajärjestelmän) kautta?

Kalasteluun liittyvissä kysymyksissä tarkoituksena oli saada mahdollisimman tarkka määrä mahdollisista riskitapauksista. Jatkokysymyksessä oli tarkoitus saada tietoon mahdollisille tie-

toturvauhkille altistumisen määrä. Haastatteluiden pohjalta yleisimmäksi tietoturvauhkaksi havaittiin etenkin sähköpostien välityksellä tapahtuva kalastelu, jossa käyttäjää yritettiin saada huijattua esimerkiksi avaamalla viestin liite. Asiakaspalvelun johto on työssään havainnut, että sähköpostisuodatin päästää toisinaan haitallisia kalasteluviestejä läpi suoraan asiakasjärjestelmän listoille. Tämän vuoksi kyseiseen asiaan haluttiin saada selkeä määrä siitä, kuinka moni työntekijä on työssään törmännyt kalasteluyrityksiin. Jatkokysymyksen perustelut ovat samat kuin edellisen kysymyksen kohdalla. Kalastelu altistaa luottamuksellisten tietojen vuotamisen väärille tahoille, kuten esimerkiksi hakkereiden tai jopa kilpailijoiden käsiin. (VAHTI 4/2013).

Yrityksen tietoturvapäällikön kanssa käydyn keskustelun pohjalta päätimme, että kalasteluun liittyvä ohjeistus toimii koulutuksen toisena pääteemana salasanakäytänteiden lisäksi.

Kysymys 12: Oletko puhunut työasioista vapaa-ajalla (esimerkiksi. Kahvilassa tai työmatkalla junassa)?

Tällä kysymyksellä oli tarkoitus kartoittaa henkilöstön tietoisuutta siitä, ettei työasioita tulisi puhua julkisilla paikoilla, jossa yrityksen tietoja olisi mahdollista salakuunnella. VAHTI- ohjeiden (4/2013) sekä yrityksen yleisten pelisääntöjen mukaisesti työasioista puhuminen julkisilla paikoilla ei ole suotavaa. Tutkija sai kuitenkin haastatteluiden pohjalta käsityksen siitä, että kyseisestä asiasta ei ole ohjeistusta henkilökunnalle. Työasioista puhuminen julkisilla paikoilla altistaa tietojen leviämisen vääriin käsiin, kuten esimerkiksi kilpailijalle.

Kysymys 13: Oletko julkaissut työhösi liittyviä asioita sosiaalisessa mediassa, kuten esimerkiksi Facebookissa?

Yrityksellä on olemassa yleiset pelisäännöt sosiaalisen median käyttöön.. Tästä huolimatta haastatteluissa kävi ilmi, että useat henkilöt ovat havainnoineet vääränlaista sekä ajattelematonta käyttäytymistä sosiaalisessa mediassa. Tämän vuoksi kohdeyksikön johto halusi saada henkilöstöltä vastauksen sosiaaliseen mediaan liittyen. Sosiaalisessa mediassa ei tulisi julkaista materiaalia työhön liittyen, koska tieto voi levitä vääriin käsiin. Tämän lisäksi sosiaalisen median kautta tapahtuva kalastelu on muodostunut erityiseksi ongelmaksi. (VAHTI 4/2010).

Kysymys 14: Selitä lyhyesti mitä tarkoitetaan termillä tietoturva?

Viimeisen kysymyksen tarkoituksena oli saada yleinen näkemys siitä, mikä on henkilöstön tietoisuus ylipäätänsä tietoturvasta. VAHTI- ohjeistuksen (4/2013) mukaisesti tämä kysymys on myös loistava tapa mitata henkilöstön motivaatiota sekä asennetta tietoturvaa kohtaan. Ky-

symykseen vastaaminen tai edes yrittäminen tarkoittaa sitä, että aihe todella kiinnostaa ja koskettaa. Mikäli kysymyksen jättää tarkoituksella tyhjäksi, voidaan määritellä, että työntekijällä ei ole edes halua paneutua tai ajatella asiaa.

3.4 Tutkimustulosten analysointi

Tutkimukseen vastasi yhteensä 97 työntekijää. Kokonaishenkilöstön määrä kuluttaja-asiakaspalvelussa on 154 henkilöä, mutta iso osa työntekijöistä on opiskelijoita. Tämän vuoksi kuukausittain laskettujen työntekijöiden määrä on 120 työntekijän verran. Tutkimuksen vastausmäärää on tämän vuoksi verrattu jälkimmäiseen lukemaan. Vastausprosentti on näin ollen noin 81%, joka kertoo sen, että otanta on erittäin hyvä antamaan yleisen kuvan kuluttaja-asiakaspalvelun henkilöstön tietoturvaosaamisen tasosta.

Tutkimustulosten päätavoitteena oli antaa vahvistus haastatteluiden sekä tutkijan havaintoihin perustetuilla epäilyksillä henkilöstön tietoturvallisesta tekemisestä. Tutkimustulokset antoivatkin lukuisia viitteitä siitä, että yleistä tietoturvakoulutusta sekä ohjeistusta ei ole esitetty tarpeeksi selkeästi. Taulukossa (taulukko 2) on analyysin perusteella arvioitu todennäköisyys uhkan toteutumiselle. Tutkija käytti analysoidessaan viitteenä VAHTI- ohjeistusta (2013) sekä tietoturvapäällikön kanssa käytyjä käytäntöjä päätetyöskentelyyn liittyen.

Yleisesti tutkimustulokset osoittautuivat suurimmalta osin juuri varsinaisten epäilyjen mukaisiksi. Etenkin kysyttäessä työnantajan tarjoamista valmiuksista (Kysymykset 1-3) havaittiin, että henkilöstöllä ei ole tarvittavaa ohjeistusta yrityksen yleiseen tietoturvaan liittyen. Haastatteluiden pohjalta tämä asia jo tiedostettiinkin kehityskohteeksi, jonka vuoksi tutkimus vahvisti epäilyksen oikeaksi. Tämän lisäksi etenkin salasanan ylöskirjoittaminen sekä työpisteen lukitseminen osoittautuivat haastatteluissa ilmenneiden epäilyksien mukaisesti negatiivisiksi.

Positiivisina yllätyksinä tutkija havaitsi muun muassa, että työpisteen salasanaa ei käytetä muissa palveluissa (Kysymys 4). Tämä selittyy helposti sillä, että yrityksen yleinen vaatimus salasanalle on niin monimutkainen (vähintään 10 merkkiä, joista yksi iso kirjain ja kaksi numeroa), että käyttäjät eivät halua vastaavia salasanoja muihin palveluihin. Toinen positiivinen asia huomattiin, ettei työkoneille ole asennettu juurikaan ylimääräisiä ohjelmia ilman lupaa (Kysymys 8). Selitys löytyy salasanan mukaisesti yrityksen sekä järjestelmänvalvojan tiukoista määritelmistä, jotka estävät suurimman osan ladatuista sovelluksista.

Erityisesti huolestuttava tulos oli tutkijan mielestä kysyttäessä työasioiden puhumisesta työpaikan ulkopuolella, jossa yhteensä noin 60 prosenttia vastanneista myönsi puhuneensa asioi-

ta ulkopuolisille (Kysymys 12). Kysymys herättää kuitenkin hieman tulkinnanvaraa, koska kysymyksessä ei oltu erikseen mainittu esimerkein mikä työasia oli kyseessä.

Toinen huolestuttava tekijä on jo epäilyksien mukaisesti ollut kalastelu eli Phishing, jota yhteensä 63 prosenttia (45 työntekijää) vastanneista oli havainnut jokapäiväisessä työssään. Yhteensä 9 henkilöä eli 20 prosenttia myönsi altistuneensa kalasteluyritykselle ja avanneensa tiedoston. Työkalun kautta saapuvia kalasteluyrityksiä oli havainnut yhteensä 61 vastaajaa, joista yhteensä 11 oli altistunut uhkalle (Kysymykset 10-11).

Tutkimuskysymykset sekä –tulokset löytyvät myös tarkasti yksilöitynä tämän opinnäytetyön liitteistä, jossa on erikseen ilmoitettu kysymyksien vastausmäärät sekä prosentit.

3.5 Uhkakuvien riskianalyysi

Mahdollisia riskejä verrattaessa tarvitaan yhteinen tapa mitata menetyksiä. Yleinen hyvä keino on määrittää jokaiselle uhkakuvalle rahallinen menetys, mikäli kyseinen uhka toteutuu. Tarkan menetyksen arviointi ei kuitenkaan ole välttämätöntä, varsinkin mikäli kyseessä on täysin eriluokan riskit. Tällöin menetyksen arvon suuruusluokka riittää varsin hyvin. Kaikille menetyksille ei ole helppo määrittää rahallista arvoa. Esimerkiksi etenkin maineen tai kilpailijalle vuodetun tiedon rahallinen arvo on erittäin vaikeasti arvioitavissa. (Courtney 1977, 99.)

Briscoen (1977, 25) mukaan riskien suuruuden määrittämiseksi tulee myös tietää taloudellisten menetysten lisäksi uhkakuvan todennäköisyys. Kvalitatiivisessa riskianalyysimenetelmässä menetyksen suuruus voidaan kuvata riittävästi sanallisesti. Tämänlaisessa kuvauksessa arvoina toimii useimmiten jokin järjestävä luokittelu, kuten esimerkiksi vähäinen – kohtalainen – huomattava.

Tutkija toteutti riskianalyysin taulukkomallina, jossa on kuvailtu tutkimustuloksissa havaitut riskit (tietoturvauhkat). Mallin arviointi tapahtui Briscoen mukaisen kvalitatiivisen riskianalyysimenetelmän mukaisesti (huomattava- kohtalainen – vähäinen). Jokaisen uhkakuvan kohdalle on myös määritelty uhkan todennäköisyys sekä prioriteetti. Prioriteetti (Erittäin tärkeä – tärkeä – huomioitava) määräytyy uhkakuvan todennäköisyydellä (huomattava – kohtalainen – vähäinen). Taulukon 2 pohjalta voidaan todeta, että punaisella merkityt uhkakuvat (kalastelu, salasanakäytännöt, sekä työpisteen lukitseminen) vaativat erityistä huomiota koulutusta suunniteltaessa. Tämän lisäksi myös muista tuloksista havaituista uhkakuvista on hyvä olla tarkennettu ohjeistus koulutuksessa, jotta uhkakuvan todennäköisyys saadaan minimoitua. Tämäntapaisten menetysten luokittelu kvalitatiivisin keinoin on huomattavasti helpompaa kuin rahallisen menetyksen arviointi, jonka vuoksi tutkija koki tämän arviointimallin riittäväksi.

Tietoturvauhka	Todennäköisyys	Prioriteetti	Koulutustarve
Kalastelu	Huomattava	Erittäin tärkeä	Kriittinen
Salasanan väärinkäyttö	Huomattava	Erittäin tärkeä	Kriittinen
Työpisteen lukitseminen	Huomattava	Erittäin tärkeä	Kriittinen
Työasioista puhuminen vapaa-ajalla	Kohtalainen	Tärkeä	Kohtalainen
Laitteen saastuminen (ulkoinen laite)	Kohtalainen	Tärkeä	Kohtalainen
Sosiaalisen median väärinkäyttö	Vähäinen	Huomioitava	Vähäinen

Taulukko 2. Uhkakuvien riskianalyysi

Tutkimustulokset antoivat selkeä kuvan siitä, mitä osa-alueita tulisi henkilöstön keskuudessa kehittää, jotta jokapäiväinen työnteko olisi turvallisempaa. Tämä toimi erityisen hyvänä motivaatiokeinona sekä tutkijalle, että yritykselle henkilöstön tietoturvaosaamisen kehittämiseksi. Etenkin kalasteluun altistuminen isolla prosentilla vaikutti huolestuttavalta, jonka vuoksi tutkija esitti tulokset viipymättä tietoturvapäällikölle välittömiä toimenpiteitä varten (Kuva 1). Riskien suuruuden määrittäminen tapahtuu tietoturvapäällikön sekä kohdeyksikön liiketoimintajohtajan välillä. Tulokset antoivat myös tietoa siitä, mitä varsinaisessa koulutuksessa on syytä käydä läpi, jotta mahdollisimman moni tietoturvauhkan todennäköisyys saadaan minimoitua.

4 Tietoturvakoulutus

Tutkijan tavoitteena oli saada tietoturvakoulutuksen avulla kehitettyä henkilöstön yleistä tietoturvatietoisuutta. Tutkija oli aikaisemmin toiminut kouluttajana muutaman projektin yhteydessä, joka helpotti koulutusprosessin suorittamista. Tietoturvakoulutuksen valmistelut tapahtuivat yhdessä yrityksen tietoturvapäällikön sekä kohdeyksikön johdon kanssa. Koulutusprosessiin sisältyi tutkijan näkökulmasta koulutusten suunnittelu, koulutuksessa käytettävän materiaalin suunnittelu sekä tuottaminen sekä varsinaisen koulutuksen toteuttaminen.

Koulutuksen suunnittelussa sekä toteutuksessa tarkoituksena on painottaa etenkin tutkimustuloksista saatua tietoa. Aikaisemmin suoritettu riskianalyysi sekä analyysin kautta saadut tiedot riskien suuruudesta edesauttoivat koko koulutusprosessin suorittamista. Koulutuksen tavoitteena on saada mahdollisimman moni havaituista uhkista minimoitua.

4.1 Tietoturvakouluttaminen sekä henkilöstön oppiminen

Tietoturvallisuuteen sitoutuminen on erityisen tärkeää etenkin henkilökunnan sekä johdon toimesta. Tämän varmistamiseksi yrityksen tulee panostaa henkilöstön tietoturvakoulutuk-

seen. Tietoturvakoulutusten tarkoituksena on parantaa tietoturvatietämyksen tasoa sekä vahvistetaan henkilöstön jokapäiväistä työskentelyä tietoturvallisuuden näkökulmasta. Kuten muuhunkin kouluttamiseen, myös tietoturvakouluttamiseen pätee yleiset lähtökohdat, joiden tulee olla kouluttajalle tuttuja. Jatkuvan osaamisen sekä ammattitaidon kehittäminen ovat olennaisia tieturvan asiantuntijuudessa. Asiantuntijana oleminen vaatii jatkuvaa kehittämistä sekä omien tietojen ja taitojen ylläpitämistä. Mikäli tieto tai taito vanhenee, asiantuntijuus kärsii huomattavasti. (VAHTI 11/2006.)

Työssä tarvitaan ammattilaisia, asiantuntijoita, mutta ei ainoastaan omalta erikoisalalta vaan myös laajalta näkökulmalta yhteisiin asioihin vaikuttavista asioista, kuten tietoturvallisuudesta. Henkilöstön perehdytys heille uskottuihin tehtäviin on johdon vastuulla. Samalla jo työtä tekevä henkilöstö tulee pitää kehitys- sekä toimintakykyisenä. Jokapäiväisten ongelmien ratkaisu sekä oman itsensä kehittäminen on tavoitteena jokaisella aikuisella. Koulutuksen tulisi tukea tätä työntekijöille olennaista piirrettä ja tarjota kehitysehdotuksia sekä uudistuksia normaaleihin työrutiineihin. (VAHTI 11/2006.)

Rogers (2004) listaa kirjassaan Aikuisoppiminen hyvän kouluttajan tunnusmerkistön seuraavasti:

”- Organisointikyky
- Sosiaaliset taidot
- Innostuneisuus
- Läsnäolevuus
- Aktivoiva opetustyyli
- Taito havaita ja ratkaista oppijan ongelmia
- Rohkeus puolustaa asiaansa
- Taito esittää monimutkaiset asiat selvästi”

Hätönen (1990) kertoo kirjassaan, koulutettavan aiheen hallitseminen olevan oleellista mikäli kyseistä tietoa opettaa eteenpäin. Ilman opetettavan aiheen hallitsemista ja tietoa kyseinen asia voidaan opettaa väärin. Vastaavissa tapauksissa ongelma ei olekaan kouluttajan taidot opettaa, vaan tiedon puutteellisuus. Kaiken tietäminen ei kuitenkaan ole kouluttajalle oleellista, koska hyvä kouluttaja oppii myös itse koulutuksessa kohdeyleisön vuorovaikutuksen avulla. Tällä tavoin tieto, taito ja kokemukset tulevat yhteiseen tietoon kaikkien saataville.

Luonnollisesti paras kouluttaja hallitsee opetettavan asian sisällön ja osaa jakaa tietoaan opetusmuodossa muille. Vastakohtana toimii kouluttaja, joka ~~osaa~~ johtaa kohdeyleisönsä harhaan. Koulutettavien asioiden sujuva hallinta on onnistuneen koulutuksen tärkein asia. Erilaisten tilanteiden hahmotus sekä kouluttajan joustavuus ovat hyvän kouluttajan edellytyksiä.

Yksi oleellinen asia kouluttajan opetustyypissä on se, millainen oppija kouluttaja itse on. Oman oppimistyylin tietäminen sekä tunteminen sekä tämän huomioon ottaminen kouluttamisessa on hyvän kouluttajan tunnusmerkistöä. Kouluttaja voi kehittää omia opetustaitojaan sekä kohderyhmän oppimista. Tähän kannattaa myös kiinnittää huomiota omassa kehityksessään kouluttajana. (VAHTI 11/2006.)

Kouluttamiselle löytyy selkeä tarve tietoturvatietoisuuden lisäämiseksi. Organisaation tehtäviä voi hoitaa vakituisen henkilöstön lisäksi esimerkiksi yhteistyökumppanit kuten palvelun toimittajat tai yrityksessä toimivat harjoittelijat. Organisaation tietoturvakäytänteiden perusteellinen perehdyttäminen on etenkin näille sidosryhmille erittäin tärkeässä asemassa. (VAHTI 11/2006.)

VAHTI- tietoturvakouluttajan oppaan mukaan (2006) nykyinen peruskäsitys oppimisesta on uuden asian oppiminen omien olemassa olevien tietojen ja taitojen lisäksi. Tärkein asia uuden asian oppimiseksi on yksilöiden kyky luoda ennakkokäsityksiä. Tämä voi johtaa siihen, että aikaisemmin opitut taidot ja tieto voivat toimia joko esteenä uuden oppimiselle tai olla oppimisen perus edellytys. Etenkin vanhat tavat sekä tieto voi estää uuden oppimista, mikäli opittava aihe on niihin huomattavassa ristiriidassa. Ihmiset keräävät iän myötä yhä enemmän ja enemmän vakituisia toiminta- ja ajattelumalleja elämänkokemuksensa myötä. Tämän vuoksi oppiminen usein rinnastetaankin vanhan tiedon tai taidon ”päivittämisestä” eli poisoppimisesta. (VAHTI 11/2006.)

Oppimisessa voi olla huomattavaa poikkeusta eri työntekijöiden kohdalla. Tähän vaikuttaa työntekijän elämänkokemus sekä tieto ja taito yrityksen toimintamalleista. Tämän vuoksi oppimistulokset voivat olla erilaisia, vaikka jokaiselle työntekijälle järjestettäisiin täysin samanlainen koulutus. Aikaisemman kokemuksen tai tiedon puute on tärkeässä roolissa oppijan kannalta. (VAHTI 11/2006.)

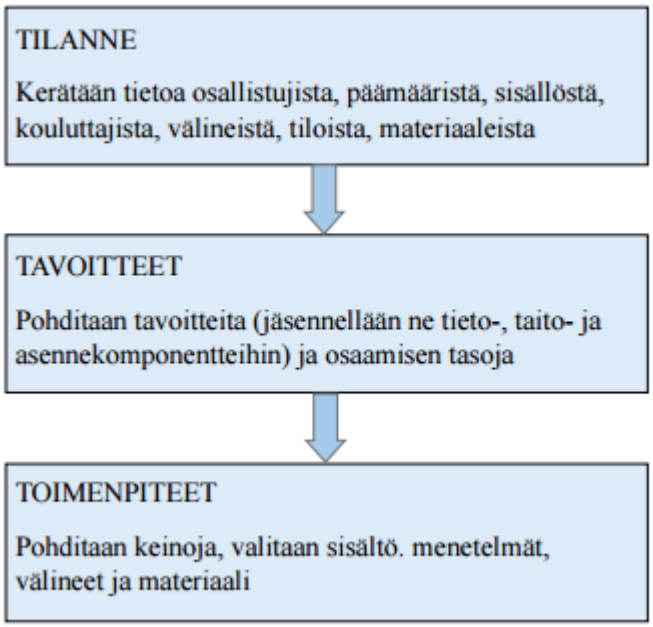
4.2 Koulutuksen suunnittelu

Valtiovarainministeriön VAHTI- tietoturvakouluttajan käsioppaan mukaan hyvä koulutussuunnitelma perustuu lyhyen ja pitkän aikavälin koulutukseen. Koulutuksissa otetaan huomioon niin yleiset kuin kohdennetut asiat. Suunnitelma tapahtuu organisaatiossa, jossa koulutustarpeet tulisi selvittää hyvän suunnitelman laatimiseksi. Suunnitelma toimii viitekehyksenä varsinaiseen koulutustoimintaan . (VAHTI 11/2006.)

Tavoitteiden asettaminen, kohderyhmän tieto-taito, käytettävä aika ja tila tulee ottaa huomioon koulutustilaisuuden suunnittelussa (Kuva 3). Tämän lisäksi kouluttajan tulee myös

suunnitella koulutusmenetelmät. Opillisesti oikea koulutus tarjoaa henkilöstölle tarvittavat edellytykset jokapäiväisten tehtävien sekä vastuiden hoitamiseen. Paras tapa mitata tietoturvakoulutusten onnistumista on se, miten hyvin koulutuksessa käydyt asiat tapahtuvat henkilöstön toimesta jokapäiväisessä työssä. (Peltonen ym. 1985.)

Ryhmäkoolla koetaan olevan ratkaiseva merkitys koulutukseen osallistuvan kohderyhmän aktiivisuudessa. Menetelmien valinnassa onkin syytä ottaa huomioon ryhmäkoko, koska liian iso ryhmä voi asettaa haasteen ryhmän uskallukselle puhua ja ottaa osaa keskusteluun. Kohdeyleisön rohkaiseminen sekä opetusmenetelmien valitseminen vaikuttavat huomattavasti vuorovaikutteiseen kouluttamiseen. Tämä on myös asia, joka hyvän kouluttajan on otettava huomioon. Vuorovaikutteinen, kohdeyleisön osallistumista vaativa luentomalli toimii oikein järjestettynä hyvin tietoturvakoulutukseen. Kehittynyt kouluttaja voi kuitenkin miettiä myös muita mahdollisuuksia, kuten esimerkiksi ryhmätyöskentelyä tai demonstraatiota. Kouluttajalla on vapaat kädet koulutusmenetelmien käytössä, kunhan koulutus pysyy suunnitelmassaan. (Uusikylä 2000, 15.)



Taulukko 2 Opetuksen suunnitteluprosessi (Peltonen 1985)

Tietoturvakouluttajan haasteena on viestin perille saaminen, jonka vuoksi koulutus on suunniteltava siten, että ensimmäisenä koulutukseen osallistuville henkilöille saadaan tietoon koko koulutuksen sanoma eli asian ydin. Tämän jälkeen kouluttajan tehtävä on herättää mielikuvia osallistujissa, joka edesauttaa oppijaa muodostamaan kokonaisuuden asiasta. Kokonaisuuden hahmottaminen tarkoittaa opittavan asian ymmärtämistä. (VAHTI 11/2006, 33.)

Riskianalyysitaulukossa (Taulukko 2) on merkitty koulutustarpeet tärkeysjärjestykseen, jonka avulla tutkija pystyy suunnittelemaan varsinaisen tietoturvakoulutuksen materiaalin yhdessä tietoturvapäällikön kanssa. Suunnittelu tapahtui yhteensä kahdessa eri tapaamisessa. Tutkimuksen tulokset toimivat hyvänä viitteenä siitä mitä asioita varsinaisissa koulutuksissa tulisi painottaa. Ensimmäisessä tapaamisessa tietoturvapäällikkö neuvoi mihin asioihin tietoturvakoulutuksessa kannattaa erityisesti panostaa. Toinen tapaaminen järjestettiin koulutusmateriaalin valmistuttua, jolloin tutkija piti koulutuksen suoraan tietoturvapäällikölle ikään kuin kenraaliharjoituksena. Tämän jälkeen tutkija sai palautteen pidetystä koulutuksesta, jonka avulla tutkija pystyi suunnittelemaan koulutuksen loppuun tehokkaasti. Tutkijan tarkoituksena oli saada selville tietoturvapäällikön avustuksella tehokas, mutta samalla kattava koulutus aikaiseksi.

Tutkija oli havainnut kohdeyksikössä, että henkilöstöön kuului varsin suuri määrä eri-ikäisiä ihmisiä. Ikähaitari toimi 18-63 vuoden ikävälillä. Tämän seikan vuoksi, koulutuksen suunnittelussa tuli ottaa huomioon henkilöstön eri taito- sekä tietotasot. Tämän vuoksi tietoturvapäällikkö sekä tutkija päättivät, että koulutukset pidetään live-koulutuksina, johon varataan kerrallaan 10-15 ihmistä ja noin tunti aikaa. Varsinainen koulutus tapahtuisi vuorovaikutteisesti, jolloin yleisöllä on koko koulutuksen ajan mahdollista esittää kysymyksiä tai liittyä keskusteluun. Tutkijan laaja tietotaito kohdeyksiköstä toimii hyvänä keinona kuvailla tietoturva-asioita käytännössä henkilöstön jokapäiväisessä työssä. Tutkija suunnittelikin koulutuksen siten, että jokainen asia oli selitettävissä kohdeyksikköä koskevin esimerkein. Tämä edesauttaa yksilöiden oppimista sekä asioiden sisäistämistä.

4.3 Koulutuksen materiaali

Kohderyhmien eroavaisuus on kouluttajan peruskysymys. Tämä tulee ottaa huomioon suunnittelussa pohtien, minkälaisia asioita erilaisten kohderyhmien kanssa tulisi käydä läpi. Samanlaisia kohderyhmiä ei juuri ole, jonka vuoksi yleistä ohjetta tai selitystä ei ole saatavilla. Kouluttajan täytyy suunnitella koulutus itse ja pohtia kannattaako koulutuksessa käydä läpi ainoastaan tiettyjä asioita syvällisemmin vai tulisiko koulutuksessa käydä läpi useampia asioita kerralla. Tietoturvatietoisuuden sekä -osaamisen ylläpitämisessä käytetään usein muitakin keinoja pelkän kouluttamisen sijaan, kuten esimerkiksi auditointeja. Auditoinnissa ulkopuolinen henkilö testaa henkilöstöä esimerkiksi vierailemalla kohdeyksikössä. Auditoija yrittää havaitsemalla arvioida henkilöstön työskentelyä. (VAHTI 11/2006.).

Tietoturvakoulutuksen materiaali tuotettiin yhdessä tietoturvapäällikön kanssa. Materiaalin viitekehyksenä toimii VAHTI- henkilöstö tietoturvaohjeistuksen mukaiset asiat sekä tutkimuslomakkeessa havaitut uhkat, jotka henkilöstöä koskevat. Materiaali suunniteltiin siten, että se olisi mahdollisimman helppolukuinen henkilöstön iästä riippumatta. Tutkija suunnitteli mate-

riaalit pääosin juuri haastatteluiden sekä havaintojen perusteella. Live-koulutuksen materiaali löytyy tämän opinnäytetyön liitteistä (Liite 2).

Riskianalyysin sekä tutkimustulosten pohjalta koulutusmateriaalin suunnittelu sekä toteutus helpottuivat huomattavasti. Riskianalyysi antoi kuvan siitä, mitkä uhkat olivat kohdeyksikössä suurimmat. Suurin osa uhkista liittyi juuri henkilöstön käyttäytymiseen, jonka vuoksi kattavalla tietoturvakoulutuksella sekä hyvin suunniteltu materiaali edesauttavat tietoturvauhkien ehkäisemisessä (Taulukko 1).

Tietoturvapäällikkö sekä tutkija tulivat yksimieliseen päätökseen siitä, että etenkin tietoturvauhkia Kalastelu (Phishing) sekä Sosiaalinen Manipulointi (Social Engineering) on hyvä tehostaa koulutusmateriaalissa. Tämän lisäksi yrityksellä on olemassa loistava ohjeistus hyvien salasanojen ”parhaista käytännöistä”, jotka on tarkoitus tuoda loppukäyttäjän tietoisuuteen (Liite 3). Kohdeyksikössä tutkija on haastattelemalla havainnut, että kerran kolmessa kuukaudessa vaihdettavat salasanat ja niiden monimutkaisuus aiheuttavat erittäin haastavia tilanteita uusien salasanojen luomiseksi. Tämän vuoksi koulutusmateriaaliin tulee kokonaan osa, jossa neuvotaan työntekijöitä luomaan uniikkeja, mutta helposti muistettavia salasanoja. Tämän lisäksi kohdeyksikön johdolta tuli pyyntö, että materiaali sisältäisi yrityksen yleisiä sääntöjä sekä ohjeistuksen Sosiaalisen Median käyttäytymiseen. Näihin asioihin panostaminen vahvistui entisestään tutkimustuloksia analysoidessa, jossa tutkija huomasi, että juuri kohdeyksikön johdon esille tuomat asiat korostuivat tuloksissa. Tämä vahvisti aiemmin suoritetun riskianalyysin arviot oikeaksi.

Luokkakoulutusmateriaali tuotettiin PowerPoint-mallina, jossa kiinnitettiin huomiota tekstin määrään sekä visuaalisuuteen. Monen rivin leipätekstin sijaan tutkija kertoi pääasiat, jotka selitettiin esimerkein auki henkilöstölle. Tämän lisäksi visuaalisuuteen panostettiin erilaisten kuvien tai kuvioiden muodossa, jotta oppija ei koe koulutusta tylsänä. Ohjeen sekä suosituksen tästä tavasta tutkija sai suoraan yrityksen tietoturvapäälliköltä, joka on pitänyt koulutuksia aikaisemmin. Tietoturva aiheena on varsin raskas, jonka vuoksi visuaalisesti hyvin tuotettu materiaali mahdollistaa oppimisen helpommaksi.

Tutkija ehdotti itse monimuotoisen materiaalin tuottamista ja tämä otettiin kohdeyksikössä erittäin hyvin vastaan, koska henkilöstö on eri-ikäistä ja vaihtuvuutta tapahtuu jatkuvasti. Materiaali suunniteltiin yhteensä kolmeen eri malliin: Luokkakoulutuksissa esitettävään malliin, uusien työntekijöiden koulutusmateriaaliksi sekä kohdeyksikön omille sivuille, josta tietoturvaohjeistus on aina helposti saatavilla ja luettavissa. Materiaalista tehtiin yhteensä kaksi luonnosta, jotka tutkija esitteli tietoturvapäällikölle. Samalla tutkija sai palautetta materiaalista sekä kehitysehdotuksia, jotka otettiin huomioon viimeistä versiota varten. Materiaalin

hyväksymisen jälkeen tutkija esitti materiaalin vielä kohdeyksikön johdolle, jossa materiaali hyväksyttiin viimeisen kerran ennen henkilöstön tietoturvakoulutuksia.

4.4 Koulutuksen toteutus

Koulutusten tavoitteena oli saada aikaan toimiva ja tehokas koulutus, jossa tutkija toimi vuorovaikutuksessa henkilöstön kanssa. Tutkija halusi saada ryhmässä aikaan keskustelua sekä oivalluksia siitä, että asioita voidaan hoitaa tavalla, jolla niitä ei ole osattu aikaisemmin katsoa. Tämän vuoksi koulutukset järjestettiin Live-koulutuksina, jolloin vuorovaikutukseen olisi paras mahdollisuus. Kohdeyksikön johto piti kirjaa siitä, että jokainen työntekijä osallistuu koulutukseen ennemmin tai myöhemmin, jotta koko henkilöstölle on saatavissa sama tieto yrityksen tietoturvakäytännöistä.

Ensimmäisen koulutuksen tutkija piti suoraan kohdeyksikön johtoryhmälle, jossa materiaali käytiin läpi perusteellisesti. Tutkija rohkaisi heti alusta alkaen vuorovaikutteiseen koulutukseen, jossa tarkoituksena oli saada mahdollisimman monipuolisia mielipiteitä materiaalissa käytävistä asioista. Koulutus toimisi samalla ikään kuin harjoituksena varsinaisia koulutuksia varten. Tutkija painotti koulutuksen edetessä, että kyseinen koulutus ei ollut ainoastaan vain työntekoa varten vaan saatavaa oppia pystyy käyttämään myös vapaa-ajalla hyödyksi.

Tietoturvakoulutukset toteutettiin kohdeyksikössä viikoittaisten tiimipalaverien yhteydessä. Kohdeyleisön koko on 10-15 henkilöä riippuen arkivapaista sekä mahdollisista sairastapauksista. Tämän lisäksi tavoitteena oli tuoda esiin koulutusmateriaalissa käytävät asiat läpi esimerkkien kautta. Esimerkit koostuivat henkilöstön jokapäiväisistä työtehtävistä. Koulutukset kestivät kohdeyleisön aktiivisuudesta riippuen 45 minuutista tuntiin. Koulutuksen lopussa materiaalin jälkeen varattiin vielä aikaa erikseen kysymyksille sekä yleiselle keskustelulle.

Koulutukset sujuivat erittäin hyvin, jonka lisäksi tutkija sai aikaan huomattavaa keskustelua aihealueista. Koulutuksien aikana kohdeyleisö rohkeni kysymään myös suoraan kysymyksiä tai esimerkkejä tilanteista, joita materiaalissa käytiin läpi. Tutkija piti koulutukseen osallistuvista henkilöistä nimilistaa, jotta koko henkilöstö saa mahdollisuuden osallistua koulutukseen. Poissaolojen takia tutkija sopi kohdeyksikön johdon kanssa ylimääräisistä koulutuksista, jotka järjestettiin alkuperäisestä koulutuksesta poissaolleille.

4.5 Materiaalin sekä koulutuksen arviointi

Valtiovarainministeriön VAHTI- ohjeistuksen (11/2006) mukaan tietoturvakoulutuksien arviointi voidaan määritellä yhteensä neljään eri tasoon:

Ensimmäiseen tasoon lasketaan varsinaisen koulutuksen arviointi, joka on erittäin haastavaa, koska siinä tulee ottaa huomioon niin monta eri asiaa. Koulutuksessa saatava välitön palaute sekä mahdollisen kyselyn teettäminen kertoo koulutukseen osallistujien ensimmäiset mietteet siitä, oliko koulutus hyvä tai hyödyllinen. Tämänlaisella palautteella voidaan vaikuttaa kouluttajan keinoihin käydä asioita läpi. Esimerkiksi materiaalin selkeys sekä kouluttajan ulosanti on mahdollista mitata helpostikin, jonka takia myös näiden asioiden kehittäminen saadun palautteen kautta on helpompaa.

Toisena tasona on huomattavasti haastavampi arviointi, joka liittyy koulutukseen osallistujien oppimiseen. Varsinaista oppimista sekä asioiden omaksumista on erittäin hankala arvioida ilman erillistä testiä tai kirjallista tenttiä. On kuitenkin mahdollista, että oppimista voidaan arvioida myös henkilöstön jokapäiväisen työn kautta saatavilla huomioilla.

Kolmantena tasona toimii toiminnallinen puoli, jossa arvioidaan työntekijöiden kykyä omaksumaan opittu asia käytäntöön omien työtehtäviensä kautta. Tämä arviointimalli on kahta edeltävää tasoa haastavampi, mutta havainnointi henkilöstön työnteossa tapahtuvista muutoksista toimii erittäin hyvänä mittarina.

Viimeisimpänä tasona pidetään koulutusten vaikutuksesta sekä tuloksista organisaatiossa tapahtuviin tietoturvauhkiin tai ongelmiin. Mittarina toimii lukemat tapahtuneista tietoturvaongelmista. Toinen toimiva mittari on itse henkilöstön tekemien virheiden määrä sekä tietoturvariskien ennakoinnin taidot.

Tietoturvakoulutuksien tavoitteiden saavuttamisen määrittäminen on erittäin haastavaa, mutta silti siihen kannattaa panostaa. Koulutuksien varsinaista arviointia pidetäänkin niin hankalana, että se on lähes mahdotonta yhden kouluttajan toimesta. Paras tapa mitata koulutusten onnistumista olisi havainto siitä, että miten koulutuksessa käydyt asiat näkyvät henkilöstön jokapäiväisessä työssä. Toinen erittäin hyvä vaihtoehto olisi tietoturvauhkien auditointi, joka voidaan suorittaa yrityksen sisällä. Auditointi tapahtuisi testaamalla kohdeyksikön henkilöstöä esimerkiksi tekeytymällä asiakkaaksi ja soittamalla asiakaspalvelun linjaan. Tällä keinolla testataan työntekijän toimia esimerkiksi asiakastietojen käsittelyn sekä luovuttamisen suhteen. Tämä toimisi hyvänä keinona testata yrityksen sisäistä käytäntöä asiakastietojen käsittelyssä. Toinen tapa voisi olla ulkopuolisen testaajan vierailun muodossa, jossa testaaja suorittaa havainnoinnin kautta arvioita henkilöstön toimista. (VAHTI 11/2006.)

Kouluttajan itse olisi hyvä kerätä välitön palaute sekä mahdolliset kehitysehdotukset omasta koulutuksestaan niin sisällön kuin ulkoisen olemuksen puolesta. (VAHTI 11/2006.)

Tärkeä asia arvioinnista tietoturvakoulutuksissa on pohtia palautteenkeruun aikaa, miksi arvioidaan ja ketä arvioidaan. Palautetta kannattaa pyytää ainoastaan mikäli oikeasti halutaan muuttaa tai kehittää asioita saadun palautteen avulla. Mahdollisimman pian koulutuksen jälkeen suoritettu palautteenkeruu on erittäin tärkeää, jotta saadaan realistinen sekä ajankohtainen mielipide koulutusten onnistumisesta. (VAHTI 11/2006.)

Opinnäytetyöprosessin aikana tutkija pyysi jatkuvasti palautetta. Tutkija sai palautetta pääosin tietoturvapäälliköltä, mutta myös kohdeyksikön johdolta (liite 4). Palautteen keruu tapahtui kahdessa palautekeskustelussa, jossa arvioitiin opinnäytetyöprosessia kokonaisuutena sekä osissa tietoturvakoulutusten sekä tuotetun materiaalin osalta. Koulutuksen materiaali tuotettiin tutkijan toimesta VAHTI- materiaalien pohjalta. Tämän lisäksi tutkija tapasi kohdeyksikön johtoryhmän sekä tietoturvapäällikön, joilta viimeinen arviointi sekä hyväksyntä tapahtui. Koulutusmateriaali arvioitiin myös suoraan loppukäyttäjien palautteen kautta, jota kerättiin koulutusten päätyttyä suoritetun kyselyn avulla. Yritys aikoo arvioida koulutusten onnistumista myös online-pohjaisella materiaalilla, johon liitetään myös erilaisia testejä ikään kuin tietoturvan ”ajokortin” merkeissä.

Toinen keino, jolla tutkija halusi arvioida työtään ja saada palautetta oli suora palautteen keruu kohdeyleisöltä eli henkilöstöltä. Palaute kerättiin välittömästi koulutusten jälkeen sähköpostitse lähetetyn online-kyselyn kautta. Palautteeseen vastattiin anonyymisti. Palautekyselyn tarkoituksena oli olla yksinkertainen, jotta vastausprosentti olisi mahdollisimman korkea. Palautetta kerättiin asteikolla 1-4, jossa pienin arvo tarkoitti vastaajan olevan täysin eri mieltä. Tämän vuoksi arvo 4 tarkoitti vastaajan olevan täysin samaa mieltä. Tämän lisäksi tutkija antoi viimeisenä mahdollisuuden avoimelle palautteelle, jossa henkilöstön oli mahdollista antaa avoimen palautteen koskien koulutusta tai kouluttajaa. Palautekyselyssä kysyttiin seuraavia asioita:

1. Koulutus oli mielestäni selkeä (3,7)
2. Koulutus oli mielestäni mielenkiintoinen (3,4)
3. Koulutus oli mielestäni tarpeellinen (3,4)
4. Koulutus antoi minulle uutta hyödyllistä tietoa (3)
5. Pystyn hyödyntämään oppimaani tulevaisuudessa (3,4)
6. Kouluttaja oli mielestäni innostava (3,5)

Kyselyyn vastasi yhteensä 114 työntekijää. Tutkija laski tutkimusvastauksista (asteikolla 1-4) . Kyselyn keskiarvot on ilmoitettu yllä mainittujen kysymysten perässä sulkeissa. Henkilöstön palautteista voidaan tulkita, että koulutus koettiin tarpeelliseksi sekä selkeäksi kokonaisuudeksi.

5 Arviointi

Opinnäytetyön arvioinnissa on otettava huomioon tehty työ kokonaisuutena. Tämän lisäksi tarkempia arviointiin huomioon otettavia seikkoja on tutkimuksen, koulutusmateriaalin sekä koulutusten suunnittelu sekä toteutus.

Palautetta kerättiin pääsääntöisesti palautekeskusteluilla sekä tämän lisäksi suoritetulla palautelomakkeella, joka oli suunnattu koulutuksiin osallistuneelle henkilökunnalle. Tutkija pyysi vielä opinnäytetyön jälkeen palautetta kirjallisesti koko prosessista, jonka avulla tutkija pystyy kehittämään omaa osaamistaan jatkossa. Kokonaisuudessaan arvioinnissa otettiin huomioon koulutuksen materiaali, itse koulutus sekä kouluttajan toimet. Tutkija pyysi palautetta opinnäytetyöhönsä liittyen kolmelta taholta: Tietoturvapäälliköltä (yhteistyö sekä tietoturvakoulutuksen materiaali), kohdeyksikön johdolta (yhteistyö sekä prosessit) sekä suoraan henkilöstön toimesta (tietoturvakoulutukset). Palautteen keruulla oli tarkoitus saada arvio tutkijan toimista koko opinnäytetyöprosessin ajalta.

Tutkijan mielestä koko tutkimus- sekä kehitysprosessi toimi erittäin sujuvasti. Säännölliset tapaamiset sekä jatkuva yhteydenpito tietoturvapäällikön sekä kohdeyksikön välillä edesauttoivat opinnäytetyön läpiviemistä. Tämä edesauttoi myös tutkijan omaa oppimista.

6 Pohdinta ja yhteenveto

Opinnäytetyön tarkoituksena oli tutkia ja kartoittaa kohdeyksikön henkilöstön tietoturvatietoisuutta sekä kehittää tutkimustulosten pohjalta kohdeyksikössä havaittuja tietoturvauhkia koulutusten avulla. Opinnäytetyötä voidaan pitää hyötynä yritykselle, jolle henkilöstön päätetyöskentelyn tietoturvallisuuteen panostaminen oli jo valmiiksi suunniteltuna kehityksen kohteena. Yrityksen hyötynäkökulman lisäksi tietoturvakoulutuksista on hyötyä myös henkilöstölle niin työelämässä kuin työpaikan ulkopuolellakin.

Tutkimus- sekä kartoitusvaiheessa tutkija sai kuvan siitä, mitkä ovat suurimmat uhkakuvat henkilöstön keskuudessa päätetyöskentelyssä. Hyvin suunnitellut haastattelut sekä tutkimuslomake edesauttoivat tehokkaan koulutuksen suunnitteluun sekä toteutukseen. Tutkimuksen sekä koulutusten suorittamisen tarve oli työelämälähtöinen. Kartoitus ja kehitysprosessia on tarkoitus käyttää yrityksen muihinkin yksiköihin. Kuluttaja-asiakaspalvelu toimi tämän toimintamallin kokeiluna.

Valmistettua koulutusmateriaalia käytetään yksikössä tulevaisuudessa muun muassa osana uusien henkilöiden kouluttamista. Henkilöstöturvallisuuteen liittyviä uhkia oli havaittavissa

huomattavasti ennen koulutusten pitämistä. Suurin osa uhkatekijöistä koostui puhtaasti henkilöstön ajattelemattomuudesta sekä tietoturvallisen osaamisen puutteesta.

Työntekijöiden päätekäyttäytyminen sekä ajattelemattomuus edesauttavat tietoturvauhkien todennäköisyyttä. Tietoturvauhkien takana onki Valtionvarainministeriön VAHTI- ohjeistuksien mukaisesti useimmiten takana ajattelemattomuus sekä riittämätön tietotaito tietoturvaa kohtaan. Jokaisella työntekijällä on vastuu omista toimistaan, mutta samalla vastuunkantajana toimii myös työnantaja, jonka tulisi antaa valmiudet tietoturvalliseen päätetyöskentelyyn.

6.1 Tulokset ja arviointi

Tapaustutkimuksessa saatiin selville, että työntekijät eivät olleet mielestään saaneet tarvittavaa koulutusta tai tietoa siitä, miten he voivat omilla toimillaan vähentää tietoturvauhkille altistumista. Etenkin salasanojen käytössä sekä salasanakäytännöissä havaittiin puutteita, jotka voivat aiheuttaa ulkopuolisten pääsyn työpisteille. Toisena erityisen huolestuttavana seikkana voidaan pitää kalasteluyrityksille altistumista.

Tämän lisäksi tutkimustulokset antoivat tietoa siitä, että työsähköpostia oli käytetty väärin palveluihin sekä uutiskirjeiden tilaamiseen. Päätetyöskentelyssä oli tutkimustulosten mukaan myös puutteita työpisteiden lukitsemisen sekä ylimääräisten laitteiden lisäämisen suhteen. Koulutustarpeita selvitettäessä apuna toimi myös tutkijan tekemä riskianalyysi, joka koostui tutkimustulosten vastauksista.

Etenkin kahden pääteeman (kalastelu, sekä salasanakäytännöt) perusteellinen läpikäyminen koulutuksessa minimoi kyseisten uhkakuvien todennäköisyyttä. Koulutuksessa käydyt asiat muokkaavat henkilöstön ajattelutapaa tietoturvallisemmaksi, jossa otetaan huomioon päätetyöskentelyssä huomioitavat tärkeät asiat, kuten esimerkiksi työpisteen lukitseminen . Tämän vuoksi tutkijan mielestä koulutuksella sekä materiaalin jakamisella henkilöstöstä johtuvia tietoturvauhkien mahdollisuutta saatiin vähennettyä huomattavasti. Tutkija onnistui lisäämään henkilöstön tietoturvatietoisuutta sekä tehostamaan ajattelua tietoturvan näkökulmasta etenkin esimerkkejä sekä mahdollisia uhkakuvia hyväksikäyttäen.

Koulutuksien tarkoituksena oli myös jakaa tietoisuutta tietoturvallisten toimintamallien parantamiseksi sekä tietoturva-ajattelun kehittämiseksi. Tutkijan mielestä tietoturvatietoisuuden kehittäminen kohdeyksikössä oli onnistunut, koska henkilöstölle saatiin valmiiksi selkeä ohjeistus siitä, kuinka päätetyöskentelyssä tulee toimia tietoturvallisesti. Koulutusten pitäminen mahdollisti rakentavan keskustelun tietoturvallisuudesta, jossa tutkija pääsi perustelemaan sekä ohjeistamaan henkilöstöä käytännön esimerkkien kautta. Koulutusten yhteydessä

tutkija kuuli useampaan otteeseen keskustelua siitä, että, koulutuksessa käydyt asiat eivät ole edes aikaisemmin tulleet mieleen.

Koulutusten jälkeen tutkijan toteuttaman arvioinnin perusteella voidaan todeta, että henkilöstö piti koulutusta tarpeellisena sekä mielenkiintoisena. Suurin osa arviointiin vastanneista kertoi oppineensa uutta tietoa sekä pystyvät käyttämään tätä uutta tietoa tulevaisuudessa.

6.2 Opinnäytetyöprosessi ja oma oppiminen

Kokonaisuudessaan opinnäytetyöprosessi kesti noin puoli vuotta. Suurimpana haasteena oli kartoittaa kaikki mahdollinen yksiköstä, jotta yritys saisi mahdollisimman suuren hyödyn opinnäytetyöstä. Opinnäytetyön rajaus onnistui erittäin hyvin, koska tutkimuksen tekijä toimi jatkuvassa vuorovaikutuksessa yrityksen tietoturvapäällikön sekä yksikön johdon kanssa. Tämän lisäksi laaja havainnointityö vierailujen muodossa kohdeyksikön tiloissa helpottivat opinnäytetyöprosessin suunnittelua sekä läpivientiä. Nämä asiat edesauttoivat parhaaseen mahdollisen lopputulokseen, jossa opinnäytetyön tekijä sai hyvää kokemusta projektityöskentelyssä työelämässä sekä yhteistyössä eri tahojen kanssa. Samalla yritys sai suuren hyödyn opinnäytetyöstä. Yritykselle tuotettiin toimiva malli henkilöstöturvallisuuden parantamiseksi, jota on tarkoitus käyttää hyödyksi kuluttaja-asiakaspalvelun lisäksi myös muissa yksiköissä.

Opinnäytetyö valmistui alkuperäistä aikataulua nopeammin, jonka vuoksi tutkimuksen tekijä oli erittäin tyytyväinen lopputulokseen. Jatkuva vuorovaikutus sekä oman tietopohjan lisääminen opinnäytetyön edetessä olivat onnistuneita asioita. Kartoituksen lisäksi varsinaisen koulutuksen pitäminen sekä suunnittelu toivat tarvittavaa kokemusta, josta on opinnäytetyön tekijälle varmasti hyötyä tulevaisuudessa. Koulutuksiin liittyvän tietoperustan sekä pedagogiikan käsittäminen antoi mahdollisuuden oppia paljon uutta. Toiseksi erittäin positiiviseksi asiaksi tutkimuksen tekijä koki varsinaisen koulutusmateriaalin valmistamisen sekä muokkaamisen kohdeyksikön erilaisiin käyttötarkoituksiin. Kokonaisuudessaan opinnäytetyö ja siihen liittyvät prosessit olivat erittäin haastavia, mutta myös mielenkiintoisia. Opinnäytetyö oli toimi suurena hyötynä tutkimuksen tekijälle.

Kokonaisuutena opinnäytetyö oli tutkimuksen tekijän mielestä onnistunut. Etenkin tietoturvapäällikön kanssa tehty yhteistyö antoi hyödyllistä tietoa sekä taitoa hallinnollisen tietoturvan näkökulmasta. Tähän liitettynä kouluttamisen teorian sekä materiaalin tuottamisen tuomat lisähaasteet antoivat opinnäytetyöstä erittäin monipuolista hyötyä. Opinnäytetyöprosessin aikana tutkimuksen tekijä sai erinomaista kokemusta projektityöskentelystä käytännössä sekä hyödyllisiä kontakteja konsernista sekä tietoturva-alan ammattilaiselta. Opinnäytetyö ja annettu työpanos antoi yritykselle mahdollisuuden kehittää henkilöstöturvallisuuttaan. Opinnäy-

tetyöprosessi antoi myös tutkimuksen tekijälle hyvät valmiudet harjoittaa työntekoa kohti tietoturva-alan ammattilaisuutta.

6.3 Jatkotutkimuksen aiheita

Henkilöstöturvallisuuteen luotuja toimintamalleja sekä etenkin kuluttaja-asiakaspalveluun toimivia malleja voisi kehittää esimerkiksi tutkimalla asiakaskontaktien käsittelyä sekä tietojen luovutusta kontaktin aikana. Asiakaskontakteja käsitellään puhelimitse, sekä sähköisten työkalujen kautta, jonka takia tehostettu tutkimus juuri tietynlaiseen asiakaspalvelutyöskentelyyn voisi olla mahdollinen. Myös sosiaalisen median kautta sekä erilaisten pikaviestin tyyppisten asiakaspalvelukanavien tutkiminen sekä kehittäminen voisi toimia erinomaisena tutkimuskohteena.

Tämän lisäksi erilaisten asiakaspalvelumallien kuten fyysisten asiakaspalvelupisteiden henkilöstöturvallisuus voisi olla jatkotutkimuksen kohteena. Kasvotusten tapahtuvassa asiakaspalvelussa on olemassa riskejä, joita puhelimen sekä sähköisten kanavien kautta tapahtuvassa asiakaspalvelutyössä ei ole.

Lähteet

S Hirsjärvi, P Remes, P Sajavaara 1997. Tutki ja kirjoita. Helsinki: Tammi.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen Tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Courtney, R.H. jr., Security risk assessment in electronic data processing systems. AFIPS Conference Proceedings, National Computer Conference, Dallas, TX, USA, June 13–16, 1977, 97–104.

Briscoe, G.J., Risk management guide. United States Energy Research and Development Administration, ERDA 76-45/11, SSDC-11, UC- 41, Washington, DC, USA, 1977.

Rogers, J. 2004. Aikuisoppiminen. Helsinki: Finn Lectura.

Hätönen, H. 1990. Aikuisten oppiminen ja opettaminen. Kognitiivisen oppimisnäkemyksen ja toiminnan teorian soveltaminen aikuiskoulutuksessa. Helsinki: Ammattikasvatushallitus.

Peltonen, M. 1985. Koulutusoppi. Helsinki: Otava

Uusikylä, K. & Atjonen, P. 2000. Didaktiikan perusteet. Helsinki: WSOY.

Valtiovarainministeriö, VAHTI 2/2008. Tärkein tekijä on ihminen. Viitattu 13.6.2015. https://www.vahtiohje.fi/web/guest/2/2008-tarkein-tekija-on-ihminen-henkilostoturvallisuus-osana-tietoturvallisuutta

Valtiovarainministeriö, VAHTI 11/2006. Tietoturvakouluttajan opas. Viitattu 27.6.2015 https://www.vahtiohje.fi/web/guest/11/2006-tietoturvakouluttajan-opas

Valtiovarainministeriö, VAHTI 4/2013. Henkilöstön tietoturvaohje. Viitattu 13.6.2015. https://www.vahtiohje.fi/web/guest/4/2013-henkiloston-tietoturvaohje

Valtiovarainministeriö, VAHTI 7/2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Viitattu 7.6.2015. https://www.vahtiohje.fi/web/guest/7/2003-ohje-riskien-arvionnista-tietoturvallisuuden-edistamiseksi-valtionhallinnossa

Valtiovarainministeriö, VAHTI 2/2014. Tietoturvallisuuden arviointiohje. Viitattu 7.6.2015. https://www.vahtiohje.fi/web/guest/2/2014-tietoturvallisuuden-arviointiohje

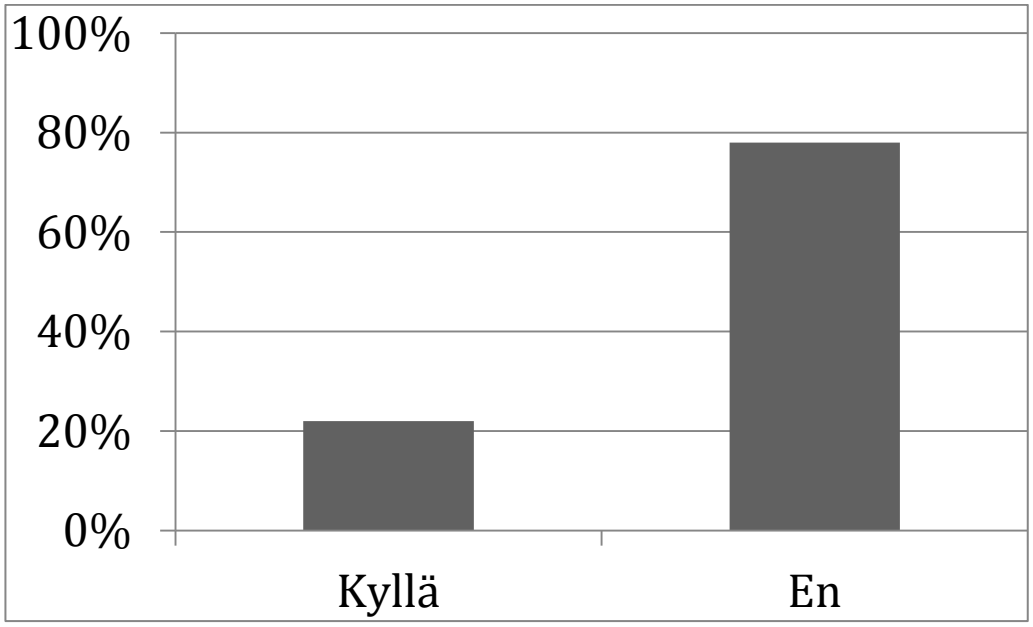
Valtiovarainministeriö, VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Viitattu 18.6.2015. https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10128&groupId=10229

Taulukot

Liitteet

Liite 1 Tutkimustulokset kysymys kysymykseltä

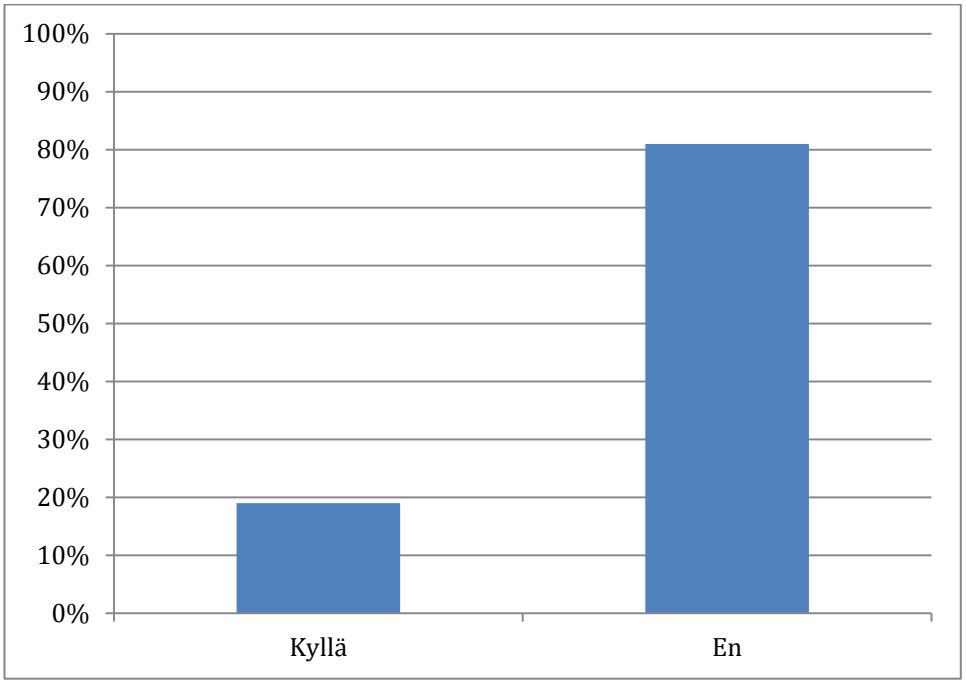
1. Oletko tietoinen yrityksen yleisestä tietoturvapolitiikasta?



Kyllä 22 %

En 78%

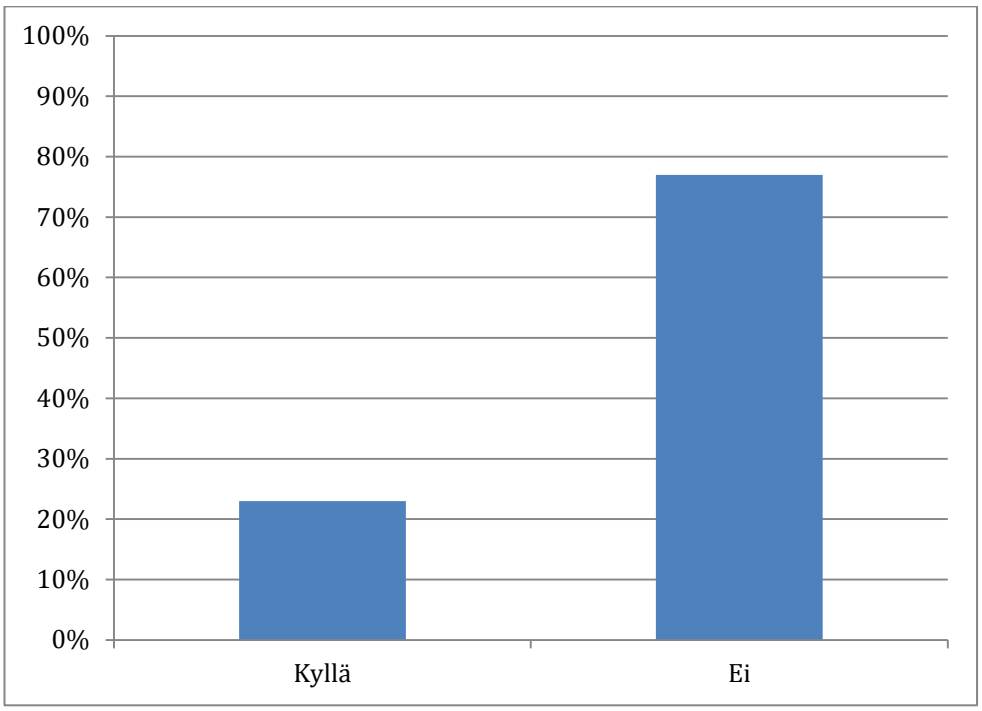
2. Oletko lukenut yrityksen yleisen tietoturvaohjeistuksen?



Kyllä 19%

En 81%

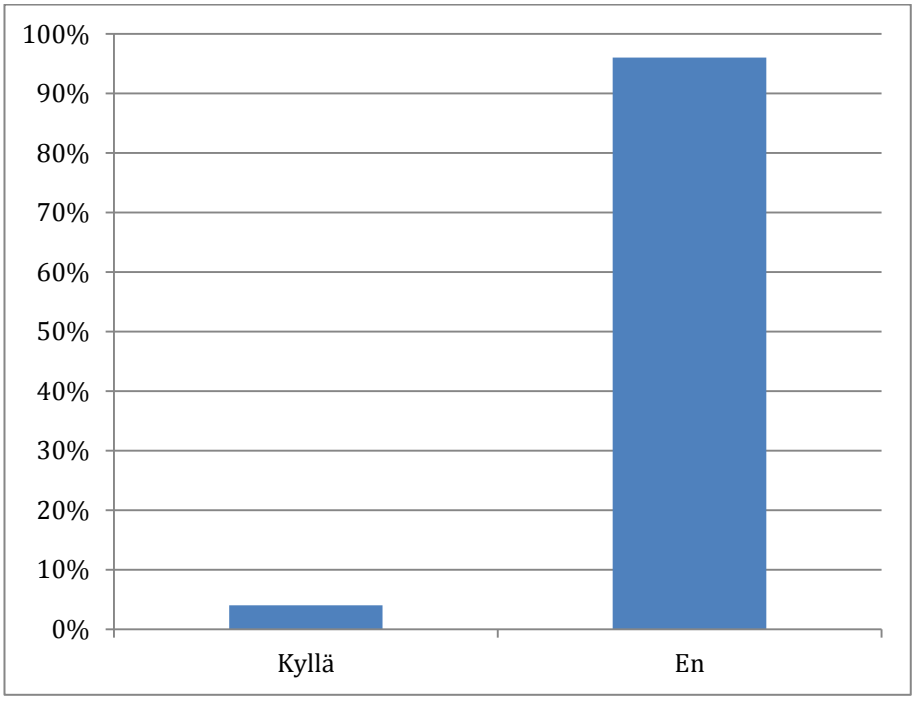
3. Onko työnantaja antanut sinulle tarvittavan ohjeistuksen tai koulutuksen tietoturvaan liittyen?



Kyllä 23%

Ei 77%

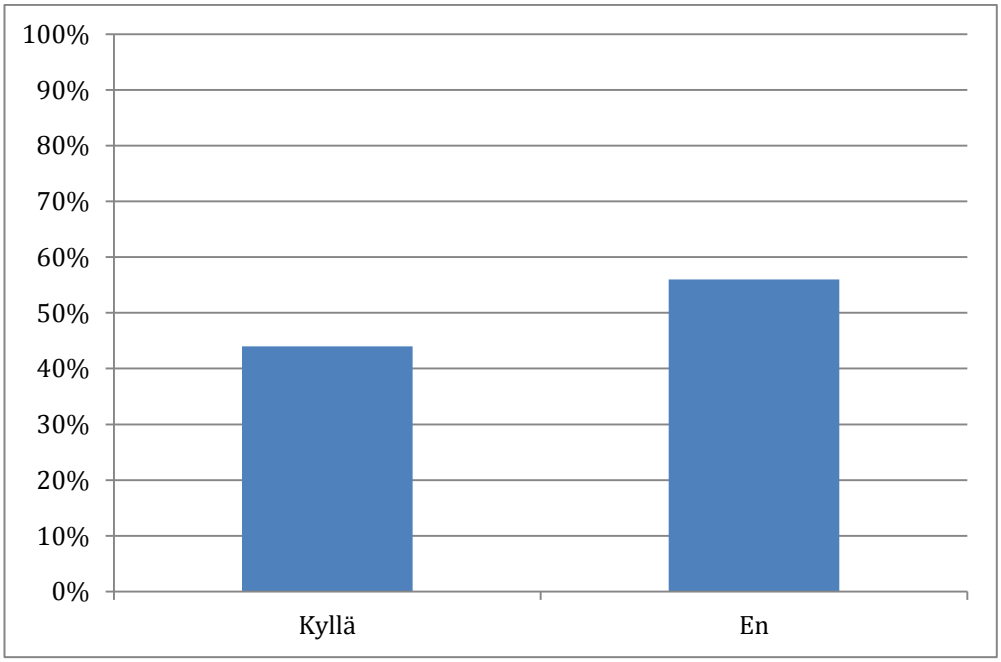
4. Käytätkö työpisteesi salasanaa myös muissa palveluissa?



Kyllä 4%

En 96%

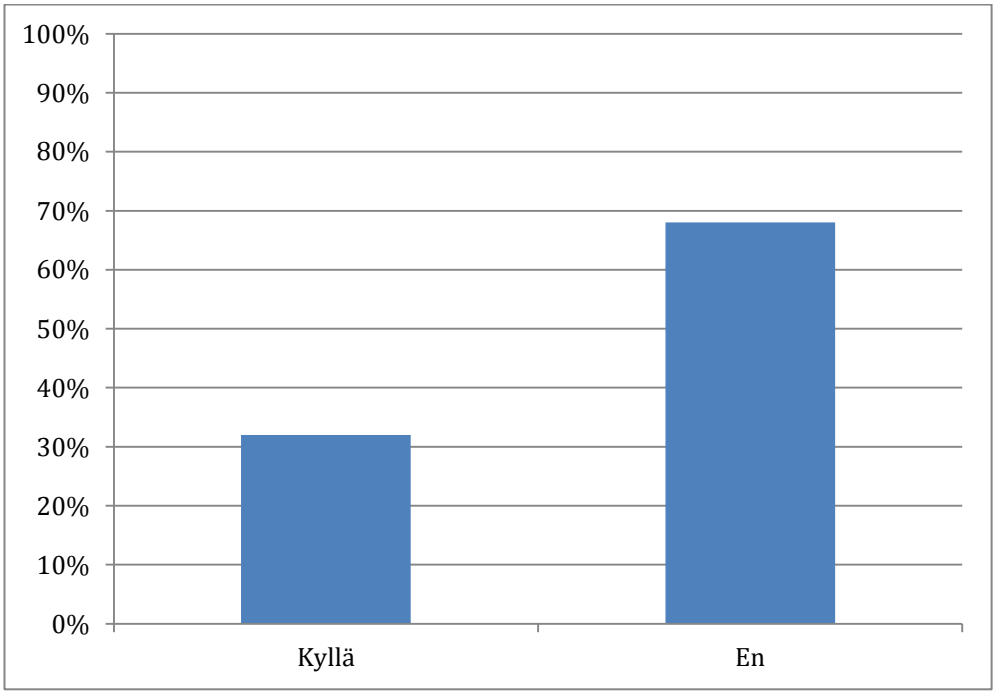
5. Oletko kirjoittanut salasanasi ylös muistiin?



Kyllä 44%

En 56%

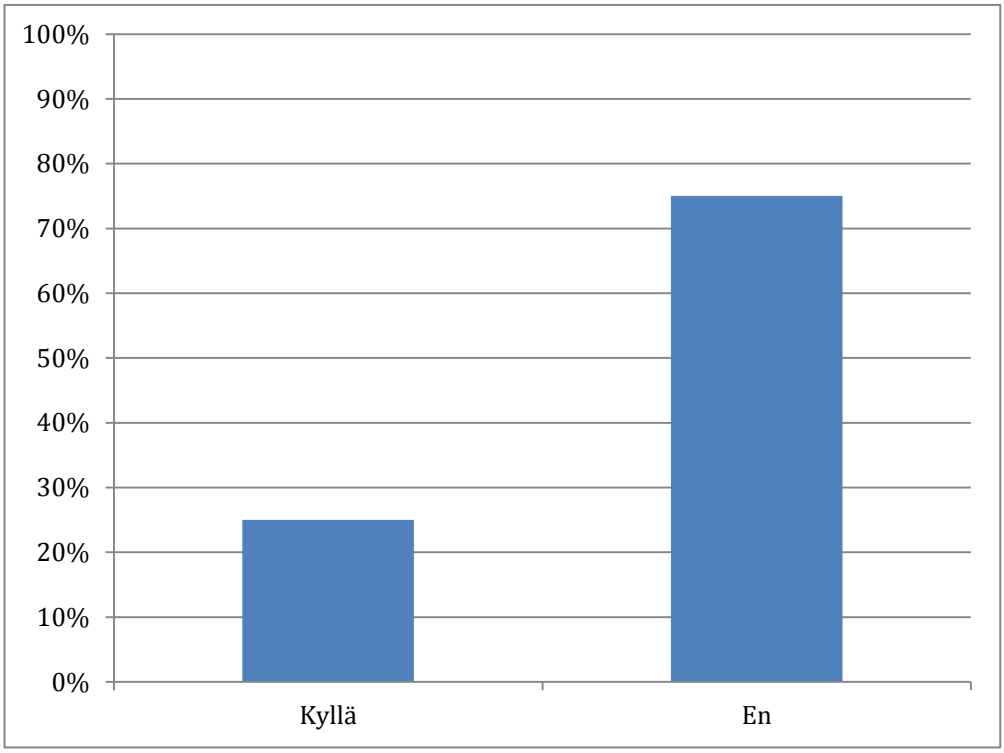
6. Lukitsetko työpisteesi aina poistuessasi paikaltasi?



Kyllä 32%

En 68%

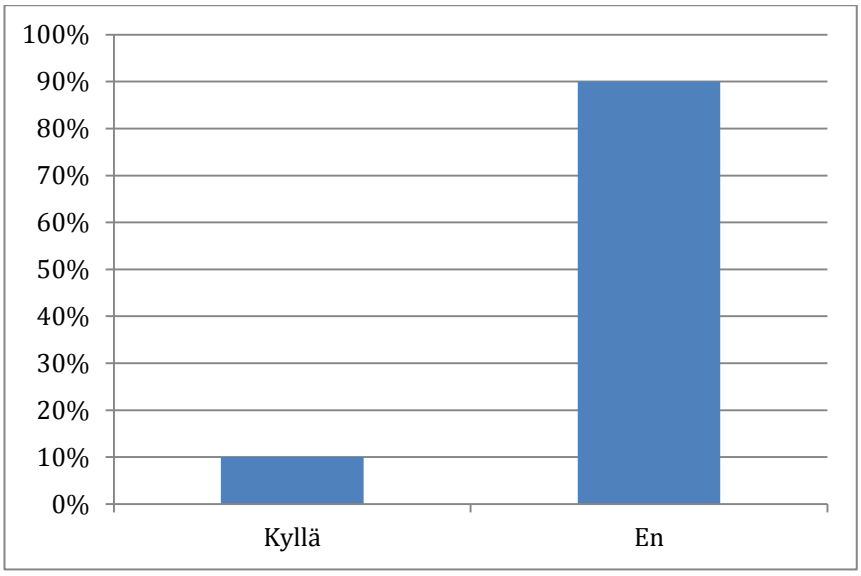
7. Käytätkö työsähköpostiasi muihin palveluihin kuten uutiskirjeisiin tai kirjautumiseen?



Kyllä 25%

En 75%

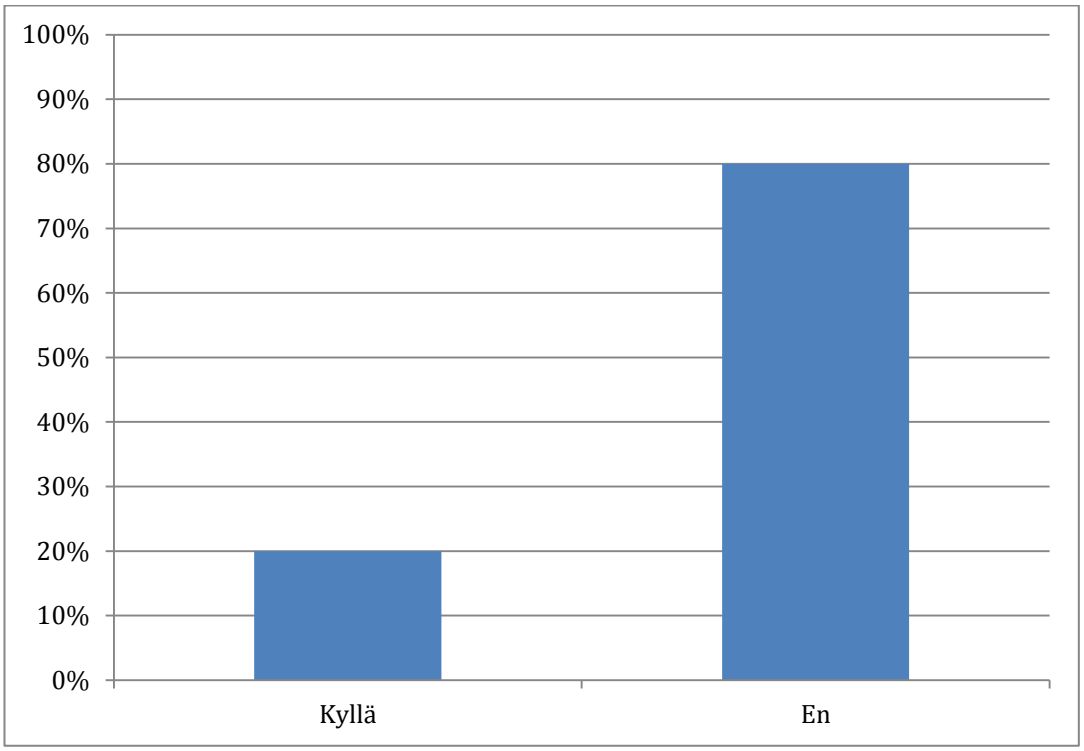
8. Oletko ladannut ylimääräisiä ohjelmia työkoneellesi?



Kyllä 10%

En 90%

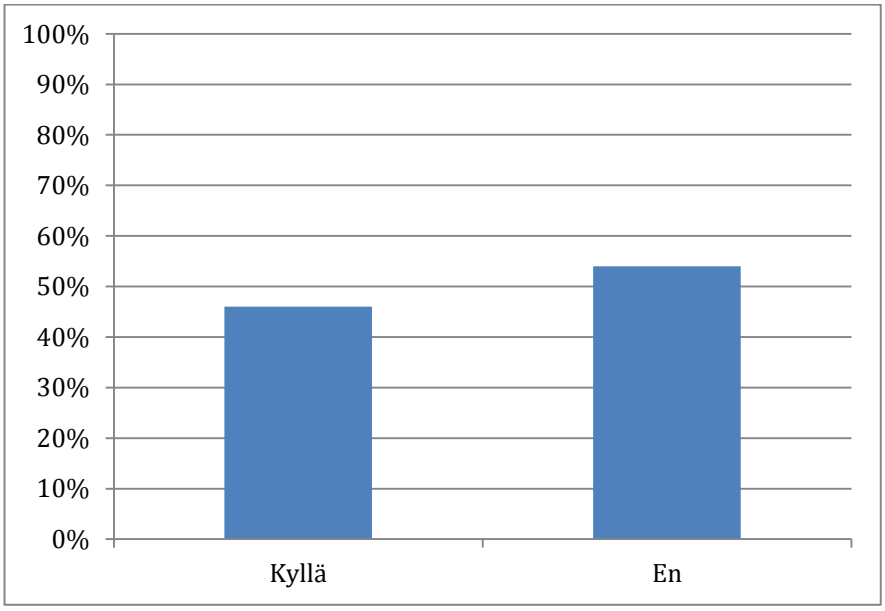
9. Oletko liittänyt ylimääräisiä laitteita työkoneellesi?



Kyllä 20%

En 80%

10. Oletko saanut työsähköpostiisi epäilyttäviä viestejä tuntemattomalta lähettäjältä?

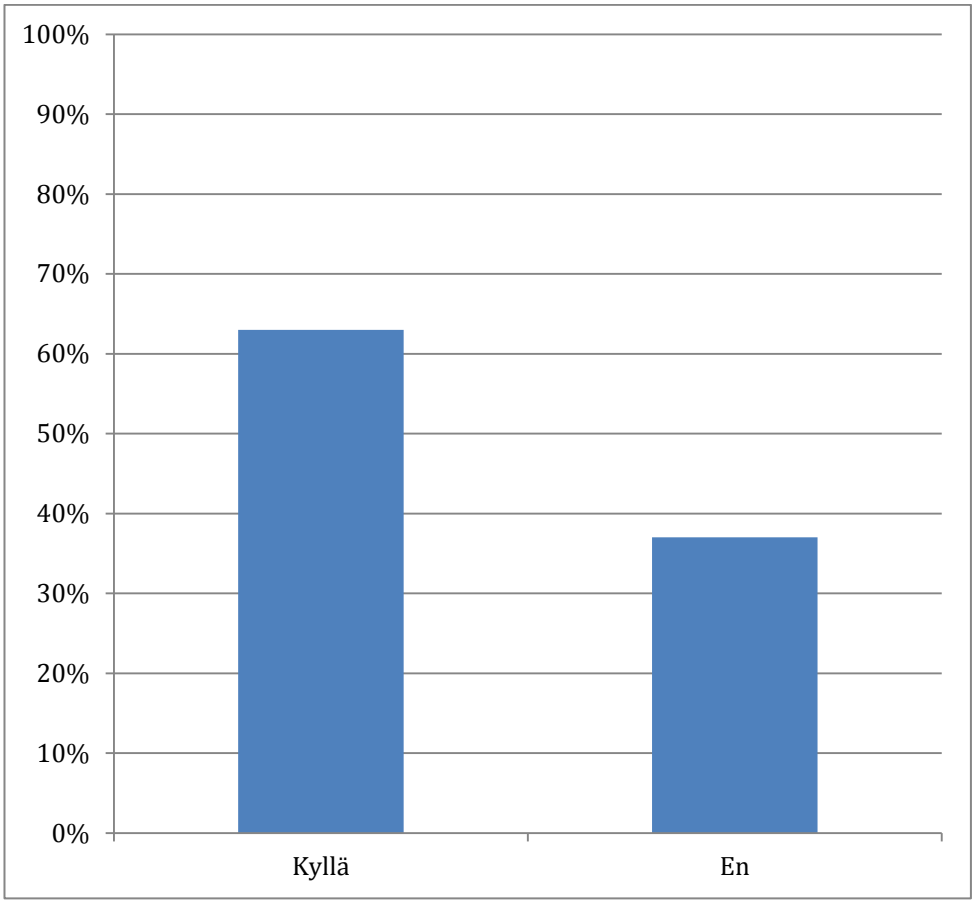


Kyllä 46%

En 54%

Jatkokysymykseen liitetiedoston avaamisesta vastasi yhteensä 39 henkilöä, joista yhteensä 9 myönsi avanneensa tiedoston.

11. Oletko törmännyt epäilyttäviin sähköposteihin yhteisen asiakashallintatyökalun välityksellä?

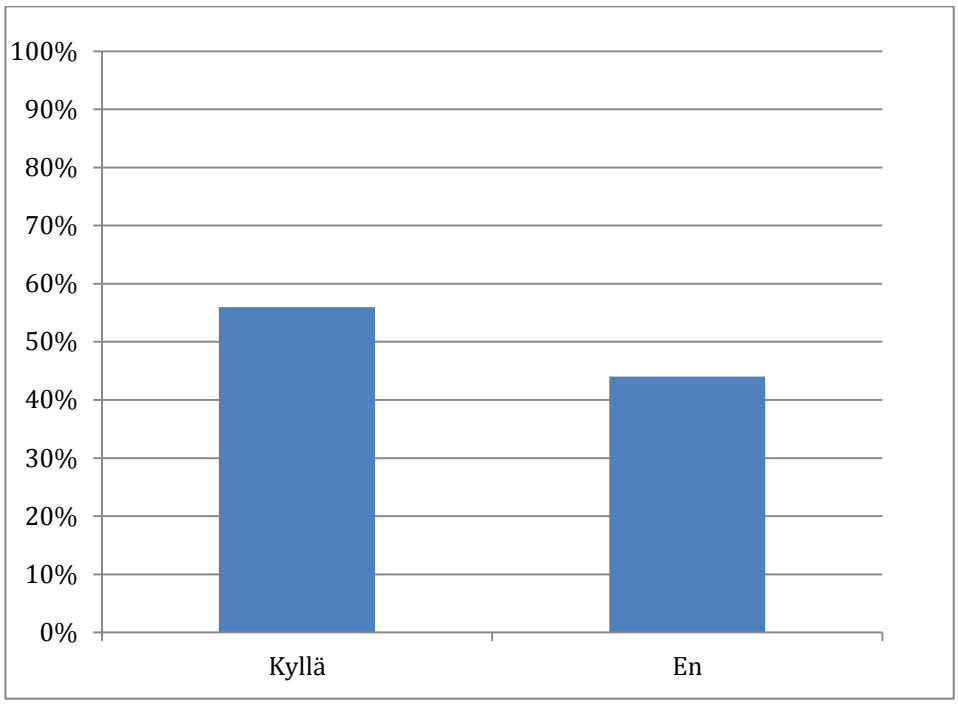


Kyllä 63%

En 37%

Jatkokysymyksessä liitetiedoston avaamisen myönsi yhteensä 11 työntekijää.

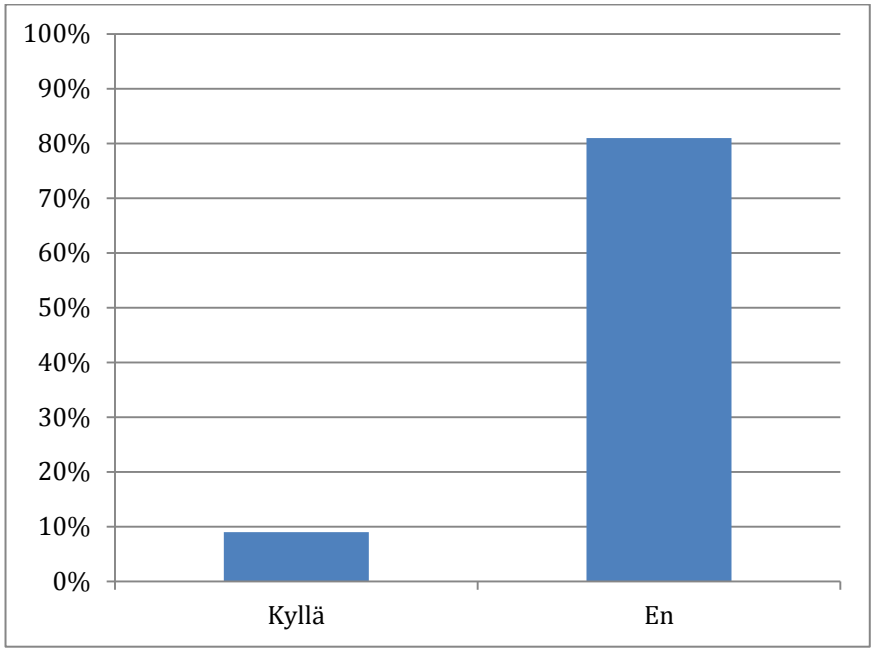
12. Oletko puhunut työasioista vapaa-ajallasi esimerkiksi ravintolassa?



Kyllä 56%

En 44%

13. Oletko julkaissut työhösi liittyviä asioita Sosiaalisessa Mediassa esimerkiksi Facebookissa?



Kyllä 9%

En 81%

Liite 2 Koulutusmateriaali

Mitä tietoturva tarkoittaa?

- Tietoturva (tai tietoturvallisuus) tarkoittaa, tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista.

- Tietoturvallisuuden osat:
  - Saatavuus -> tieto on saatavilla
  - Luottamuksellisuus ->tietoa käsittelee ainoastaan henkilöt joille se kuuluu
  - Eheys -> Tietojen ajantasaisuus

Yleinen tietoturvallinen käyttäytyminen
"House rules"

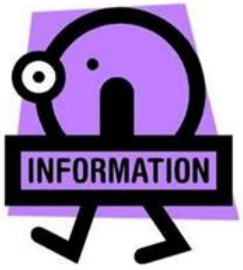
1. Lukitse työpisteesi

2. Älä liitä ylimääräisiä laitteita

3. Työsähköposti on työsähköposti

Tietojen käsitteleminen

- Älä koskaan luovuta arkaluontoista tietoa esimerkiksi sähköpostilla tai viestimissä
- Ajattele, missä ja miten puhut työhösi liittyvistä asioista
- Hävitä paperilla olevat asiakastiedot tai listat viipymättä ohjeiden mukaisesti



Salasanojen parhaat käytännöt

1. Älä käytä samaa salasanaa muissa palveluissa
2. Käytä vahvoja, uniikkeja salasanoja
3. Pidä salasanat omana tietonasi
4. Vaihda salasanasi jos epäilet väärinkäyttöä
5. Älä käytä helposti arvattavia tietoja

Kuinka luon vahvan salasanan?

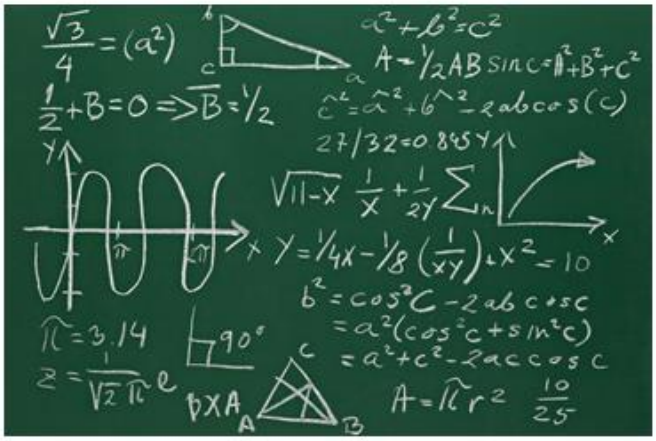
- Nykyaikainen ”salalause” salasanan sijaan
- Käytä äidinkieltäsi tai esimerkiksi slangia
- Muuta sanoja
- Koolla on väliä!

Esimerkkejä:

KukkaroMatissa?

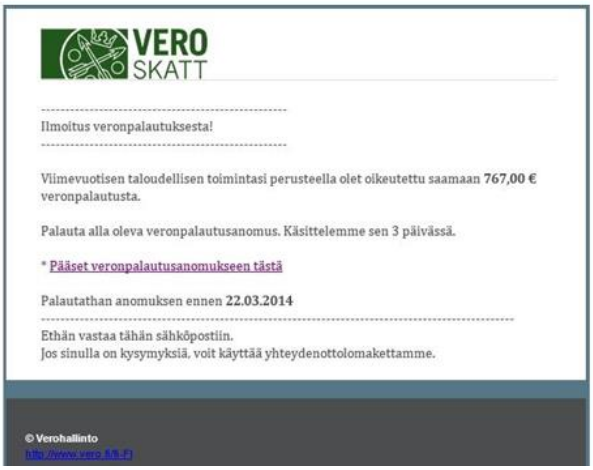
VainRaivasonTajana!

!SkaffaaTsetti



Mitä tarkoittaa?

Phishing (kalastelu)


VERO SKATT

Ilmoitus veronpalautuksesta!

Viimevuotisen taloudellisen toimintasi perusteella olet oikeutettu saamaan **767,00 €** veronpalautusta.

Palauta alla oleva veronpalautusanomus. Käsittelemme sen 3 päivässä.

* Pääset veronpalautusanomukseen tästä

Palautathan anomuksen ennen **22.03.2014**

Ethän vastaa tähän sähköpostiin.
Jos sinulla on kysymyksiä, voit käyttää yhteydenottolomakettamme.

© Verohallinto

Social Engineering (sosiaalinen manipulointi)

Kuinka tunnistan kalasteluyrityksen?

- Tuntematon lähettäjä tai sähköpostin aihe
- Kielioppivirheet
- Yleiset viestit, joissa vaaditaan välittömiä toimia
- Yleisesti kaikki yhteydenotot, joissa kysytään käyttäjätietojasi
- ”Järjettömät” tarjoukset

Lähettäjä: Info@binarypromo.club

Ajattele kahdesti ennen kuin klikkaat

- Vältä tuntemattomien linkkien tai liitteiden avaamista sähköposteissa tai viestimissä
- Älä hyväksy tai paina ”ok”-painiketta mainoksien tai tarjousten yhteydessä
- Etsi haluamasi internetosoite itse tai avaa se kirjanmerkeistäsi

Sosiaalinen Media eli ”SoMe”
”Mitä nettiin laitat, se netissä pysyy”

Sosiaalisen Median pelisäännöt

- Käytä ”maalaisjärkeä” kun julkaiset materiaalia Sosiaalisessa Mediassa
- Varmista profiilisi yksityisyys ellet halua koko maailman tietävän asioistasi
- Toimit SoMessa yksityisenä käyttäjänä, mutta edustat silti työnantajaasi
- Suojele omia sekä yrityksen tietoja

Mitä tehdä tietoturvaongelman tapahtuessa…

- Välitön reagointi on erittäin tärkeää

→ Tunnusten tai salasanan väärinkäytössä vaihda salasanasi viipymättä

- Jos havaitset väärinkäyttöä tai altistut tietoturvauhkalle ota yhteys omaan esimieheesi tai osoitteeseen xxxxxxxxxxx
- **Muistakaa**: Ei ole typeriä kysymyksiä (varsinkaan tietoturva-asioissa!)

Liite 3 Yrityksen parhaat käytännöt salasanoille

Salasanaohjeet

Salasanat ovat usein ainoa este luvattomalle pääsylle sinun henkilökohtaisiin tai yrityksen tietoihin. Sanoman ja sinun luottamuksellisten tietojen suojaamiseksi on tärkeä ymmärtää salasanojen merkitys ja miten niitä käytetään oikein.

Näissä ohjeissa kerrotaan hyviä salasanakäytäntöjä, Sanoman verkkosalasanojen tekniset vaatimukset ja annetaan vinkkejä vahvojen salasanojen muodostamiseen.

Parhaat käytännöt

- **Älä käytä työpaikan salasanoja muissa verkkopalveluissa.** Saman salasanan valitseminen vastaa saman avaimen käyttämistä kodin, auton ja toimiston lukitsemiseen – jos rikollinen pääsee käsiksi yhteen, kaikki vaarantuvat.
- **Käytä vahvoja, uniikkeja salasanoja.** Yleinen suositus on käyttää jokaisessa mahdollisessa palvelussa eri salasanaa. Käytännössä tämä voi olla työlästä, joten käytä yksilöllistä salasanaa ainakin kaikissa tärkeissä palveluissa, kuten Sanoman verkossa, pankkipalveluissa, henkilökohtaisessa sähköpostissa ja käyttämissäsi sosiaalisen median palveluissa.
- **Pidä salasanat omana tietonasi.** Älä koskaan kerro salasanojasi kenelläkään, älä edes Service Deskille. Service Desk ei koskaan kysy salasanaasi, ja jos kuitenkin kysyy niin mainitse asiasta.
- **Vaihda salasanasi, jos epäilet sen joutuneen sivullisten käsiin.** Mikäli epäilet salasanasi vuotaneen vaihda se välittömästi kaikissa palveluissa, joissa on käytetty samaa salasanaa.
- **Älä käytä salasanassa helposti arvattavia tietoja.** Älä käytä salasanoissasi mitään mikä on yleistä tietoa tai löytyy helposti sosiaalisen median profiilistasi, eli tietoja kuten syntymäpäivääsi, asuinpaikkakuntaasi, puolisosi tai lemmikkisi nimeä. Huomioithan tämän myös joidenkin verkkopalvelujen vaatimissa turvakysymyksissä!

Tekniset vaatimukset

- Salasana on vaihdettava **90** päivän välein.
- Salasana ei voi olla sama kuin jokin edellisistä salasanoista.

- Salasana ei saa sisältää käyttäjätunnusta eikä etu- tai sukunimeäsi.
- Salasanan on oltava vähintään **10** merkkiä pitkä.
- Salasanan on sisällettävä merkkejä vähintään kolmesta näistä viidestä ryhmästä:
    - ISOT KIRJAIMET (A-Ö)
    - pienet kirjaimet (a-ö)
    - numerot (0-9)
    - erikoismerkit (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
    - Merkit, jotka ovat aakkosia mutta jotka eivät ole isoja eivätkä pieniä kirjaimia. Lähinnä aasialaisten kielten merkkejä.

Huomautus: Käyttäjätili lukitaan, jos syötät salasanan väärin **viisi** kertaa **viiden** minuutin aikana. Tili kuitenkin avataan automaattisesti **viiden** minuutin kuluttua, eli tavallisesti sinun ei tarvitse olla yhteydessä Service Deskiin.

Vahvojen salasanojen muodostaminen

Käytä hetki aikaa ja yritä muodostaa salasana, joka on helppo muistaa mutta vaikea arvata:

- **Suosi salalauseita salasanojen sijaan.** Unohda perinteinen ajattelu yhdestä sanasta numeroilla jatkettuna ja valitse vaikkapa muutama sana, jotka eivät liity mitenkään toisiinsa.
- **Jos mahdollista, käytä äidinkieltäsi englannin sijaan.** Suomen kielen sanat sijamuotoineen löytyvät epätodennäköisemmin rikollisten sanakirjoista.
- **Muuttele sanoja tai kirjoita ne väärin.** Älä käytä sanojen perusmuotoja vaan lisää tai poista merkkejä, käytä eri taivutusmuotoja, murretta, sananmuunnoksia tai kirjoita jotain tahallaan väärin.
- **Mitä pidempi, sitä parempi!** Tärkein sääntö on tehdä salasanoista mahdollisimman pitkiä, mielellään yli 16 merkkisiä.

Esimerkkejä:
suomi:
KukahanKolaroiKärsämäellä?
SuperselliTakoMassii!
SevaruusAikkailu2002
hollanti:
Salarismet5%kantelen
Wat?3crocettenperweec?
MijnHuis=NietNr12@Operaplein
englanti:
Fenguage&Lather

Deside-Propaply-Sugestion

CorrectHorse@BatteryStaple

Huomautus: Ethän tietenkään käytä näitä esimerkkisalasanoja.

Liite 4 Palaute opinnäytetyöstä asiakaspalvelupäällikön toimesta

Tutkija aloitti opinnäytetyön esittelemällä tavoitteet asiakaspalvelupäälliköille. Esittelyn yhteydessä käytiin keskustelua asiakaspalvelun tietoturvaan liittyvien asioiden ymmärryksestä ko. hetkellä ja yleisistä vallitsevista toimintatavoista. Todettiin yhteisesti, että tietoturva on jo käsitteenä haastava, joten sisällön avaaminen, ymmärryksen lisääminen ja toimintatapoihin vaikuttaminen ovat ehdottomasti tärkeitä tavoitteita. Tutkija piti koko suunnitteluvaiheen ajan asiakaspalvelupäälliköt ajan tasalla materiaalin sisällöstä ja esitti myös tarkentavia kysymyksiä asiakaspalvelu kohderyhmänä huomioituna. Suunnitteluvaiheessa tutkija sai ohjausta Tietoturvasta vastaavan yksikön esimieheltä vaadittavasta osaamisen tasosta koko yrityksen osalta ja samalla myös tarpeesta asiakaspalvelun näkökulmasta. Tutkija aloitti asiakaspalvelun tietoturvan ymmärryksen tason kartoituksen erillisellä kyselylomakkeella. Saatujen tuloksien pohjalta koulutukselle oli selvästi tarvetta.

Itse koulutuksen tutkija aloitti esittelemällä koulutusmateriaalin Viikkoinfossa, jossa osallistujia olivat asiakaspalvelun johtoryhmän jäsenet, tiimien palveluesimiehet, valmennustiimi ja resurssien suunnitteluyksikkö. Materiaali ja tutkijan suullinen esitys todettiin yksimielisesti selkeäksi, tärkeitä kohtia painottavaksi ja havainnolliseksi, kun huomioidaan asiakasneuvojien laaja ikäjakauma ja erilaiset työkokemustaustat.

Asiakasneuvojien koulutus toteutettiin tiimipalavereissa, jotta osallistujaryhmän koko saatiin pidettyä n. 15 henkilössä. tutkija kävi läpi kyselylomakkeen tulokset ja sitä kautta havainnollisti selkeällä tavalla miten asiakaspalvelussa on vastattu kysymyksiin ja miksi koulutukselle on tarvetta. Tiimeistä saamani palaute on pelkästään positiivista ja koulutus todettiin todella tarpeelliseksi. Materiaali oli selkeä ja tutkijan kertomat esimerkit havainnollistivat hyvin kirjallista materiaalia.

Koulutuksessa käsiteltiin erinomaisella tavalla tietoturvaa tarpeeksi yksityiskohtaisella tasolla päivittäisessä työssä (esim. salasanat, päätteen lukitseminen, salassapitovelvoite). Nykyinen henkilökunta on tällä hetkellä koulutettu ja tarkoituksena on lisätä tutkijan tekemä koulutusmateriaali osaksi uuden työntekijän perehdytysjaksoa. Koulutusmateriaali on tarkoitus lisätä myös asiakaspalvelun omalle ohjesivustolle, jotta se on jatkuvasti henkilökunnan käytettävissä. Erinomaisesti hoidettu projekti kaikilta osin!